

Zur Zahlentheorie der Polynome

Ein Analogon zum Dirichlet'schen Satz

Inauguraldissertation

der Naturwissenschaftlichen Fakultät
der Friedrich-Alexander-Universität Erlangen

zur

Erlangung des Doktorgrades

vorgelegt von

Friedrich Grummich

aus Aussig

Berlin

Akademie-Verlag

1959

Als Dissertation genehmigt
von der Naturwissenschaftlichen Fakultät
der Universität Erlangen

Tag der mündlichen Prüfung: 27. November 1957

Dekan: Universitätsprofessor Dr. R. Fleischmann

Berichterstatter: Universitätsprofessor Dr. W. Specht

Berichterstatter: Universitätsprofessor Dr. Th. Schneider

Sonderabdruck aus „Mathematische Nachrichten“

17. Band, Heft 3—6, Januar—April 1959

Akademie-Verlag, Berlin



Zur Zahlentheorie der Polynome

Ein Analogon zum Dirichlet'schen Satz

Von FRIEDRICH GRUMMICH in Erlangen

(Eingegangen am 22. 4. 1958)

In einer Reihe von Arbeiten¹⁾ hat W. Specht die Anzahl $I_m(x)$ der irreduziblen, ganzzahligen Polynome $f(z) = z^m + a_1 z^{m-1} + \dots + a_m$, deren Koeffizienten die Normbedingung

$$a_1^2 + \dots + a_m^2 \leq x^2$$

erfüllen, asymptotisch in Abhängigkeit von der Normschränke x bestimmt. Dies ist ein Analogon zum bekannten Primzahlsatz in der Zahlentheorie der Polynome.

Vorliegende Arbeit hat das Ziel, ein entsprechendes Analogon zum Dirichletschen Satz über die Anzahl der Primzahlen einer arithmetischen Progression zu finden. Im einzelnen handelt es sich um folgende Aufgabe:

Gegeben sei eine natürliche Zahl $m \geq 2$ und zwei ganzzahlige, teilerfremde Polynome

$$B(z) = z^s + b_1 z^{s-1} + \dots + b_s, \quad 1 \leq s \leq m-1;$$

$$C(z) = c_1 z^{s-1} + \dots + c_s, \quad 1 \leq s \leq m-1.$$

Weiter seien

$$f(z) = z^m + a_1 z^{m-1} + \dots + a_m; \quad g(z) = z^r + t_1 z^{r-1} + \dots + t_r$$

ganzzahlige Polynome der Grade m bzw. $r = m - s$, welche die Bedingungen

$$(1.1) \quad f(z) \equiv C(z) \pmod{B(z)},$$

$$(1.2) \quad f(z) = B(z) g(z) + C(z)$$

erfüllen.

¹⁾ Vgl. W. SPECHT, Zur Zahlentheorie der Polynome. Sitz.-Ber. math.-naturwiss. Abt. bayr. Akad. Wiss. 1951, 139—146. — Zur Zahlentheorie der Polynome II, III. Diese Nachr. 7, 105—126, 127—150 (1952). — Zur Zahlentheorie der Polynome IV. Math. Zeitschr. 57, 291—335 (1953). Die Arbeiten werden weiterhin mit ZPI, ZPII, ZPIII bzw. ZPIV zitiert. Für das genannte Problem vgl. bes. ZPII und ZPIII.

Ferner sei unter der Norm $N(\varphi)$ eines ganzzahligen Polynoms $\varphi(z) = d_0 z^n + \dots + d_n$ der positive Wert

$$N(\varphi) = (d_0^2 + \dots + d_n^2)^{1/2}$$

verstanden. Für eine beliebige reelle positive Zahl x sei $\mathfrak{R}_{ms}(x)$ die Menge, $K_{ms}(x)$ die Anzahl der Polynome $f(z)$, welche die Kongruenz (1.1) erfüllen und deren gemäß (1.2) zugehöriges Polynom $g(z)$ der Normbedingung

$$(N) \quad N(g) = (1 + t_1^2 + \dots + t_r^2)^{1/2} \leq x$$

genügt. $I_{ms}(x)$ sei die Anzahl der (im Körper der rationalen Zahlen) irreduziblen Polynome $f(z)$ aus $\mathfrak{R}_{ms}(x)$, $R_{ms}(x)$ die Anzahl der reduziblen. Dann gilt natürlich stets:

$$(2) \quad I_{ms}(x) + R_{ms}(x) = K_{ms}(x).$$

Gesucht ist der asymptotische Wert der Anzahlen $I_{ms}(x)$ und $R_{ms}(x)$ in Abhängigkeit von der Norm x . Die Anzahl $K_{ms}(x)$ ist für jedes m gleich der Anzahl der Gitterpunkte innerhalb und auf der Oberfläche der r -dimensionalen Kugel vom Radius $(x^2 - 1)^{1/2}$, also

$$(3) \quad K_{ms}(x) = \alpha_r x^r + O(\psi_r(x)) \quad \text{mit} \quad \alpha_r = \frac{\pi^{\frac{r}{2}}}{\Gamma\left(\frac{r}{2} + 1\right)},$$

wobei $\psi_r(x)$ das Restglied des r -dimensionalen Kugelproblems bedeutet, speziell also $\psi_1(x) = 1$.

Die Ergebnisse der Untersuchung hängen in einigen Fällen von den Eigenschaften des Polynoms $B(z)$ ab. Eine von diesen unabhängige Aussage kann man nur machen, wenn s relativ klein gegenüber m ist. Diesen Fall behandelt der Hauptsatz 1. In den Hauptsätzen 2 und 3 werden die speziellen Annahmen $B(z) = z^2 + b_1 z + b_2$ bzw. $B(z) = (z - b)^s$ gemacht. Hierdurch gelingt es, die Fälle $s = 1$ und $s = 2$ vollständig zu erledigen und im übrigen die obere Grenze der Grade s , für welche der Beweis durchgeführt wird, heraufzusetzen.

Die Notwendigkeit der Fallunterscheidung bezüglich des Polynoms $B(z)$ zeigt sich vor allem darin, daß man für die Anzahl $R_{52}(x)$ verschiedene Größenordnungen erhält je nachdem, ob die Diskriminante von $B(z)$ verschwindet oder nicht. Eine Ausdehnung der angewandten Methoden auf noch größere Grade s im Spezialfall $B(z) = (z - b)^s$ führt auf recht schwierige Probleme der Eliminationstheorie, eine Ausdehnung auf andere Spezialfälle entweder ebenfalls auf eliminationstheoretische Probleme (z. B. im Fall eines reduziblen $B(z)$ mit verschiedenen Faktoren) oder außer diesen auf Probleme der algebraischen Zahlentheorie (z. B. im Fall eines irreduziblen $B(z)$ vom Grade $s \geq 3$).

Zur besseren Formulierung der erhaltenen Ergebnisse sei folgende Feststellung getroffen: $\mathfrak{T}(B, C)$ sei die (endliche) Menge der ganzen Zahlen z , für welche die gebrochene Funktion $\frac{C(z)}{B(z)}$ ganzzahlige Werte annimmt, während die Zahlen $\beta_n(B, C)$ für $n \geq 1$ definiert seien durch:

$$(4) \quad \beta_n(B, C) = \sum_{u \in \mathfrak{T}(B, C)} (1 + u^2 + \dots + u^{2n})^{-1/2}.$$

Dann gilt der

Hauptsatz 1. Die Anzahl der reduziblen bzw. der irreduziblen Polynome $f(z)$ aus $\mathfrak{R}_{ms}(x)$ ist bei beliebigem Polynom $B(z)$:

$$(5.1) \quad R_{21}(x) = O(1)$$

$$(5.2) \quad I_{21}(x) = \alpha_1 x + O(1)$$

$$(5.3) \quad R_{31}(x) = \alpha_1 \beta_1(B, C) x + O(1)$$

$$(5.4) \quad I_{31}(x) = \alpha_2 x^2 - \alpha_1 \beta_1(B, C) x + O(\psi_2(x))$$

$$(5.5) \quad R_{32}(x) = O(1)$$

$$(5.6) \quad I_{32}(x) = \alpha_1 x + O(1)$$

$$(5.7) \quad R_{ms}(x) = \alpha_{r-1} \beta_{r-1}(B, C) x^{r-1} + O(x^{r-2})$$

$$(5.8) \quad I_{ms}(x) = \alpha_r x^r - \alpha_{r-1} \beta_{r-1}(B, C) x^{r-1} + O(\psi_r(x)) \quad \left. \vphantom{\begin{matrix} (5.7) \\ (5.8) \end{matrix}} \right\} \text{ falls } s \leq \frac{m-3}{2}.$$

Weiter gilt der

Hauptsatz 2. Die Anzahl der reduziblen bzw. irreduziblen Polynome $f(z)$ aus $\mathfrak{R}_{m2}(x)$ ist, falls $B(z) = z^2 + b_1 z + b_2$ mit $\Delta = b_1^2 - 4b_2 \neq 0$:

$$(6.1) \quad R_{12}(x) = \alpha_1 \beta_1(B, C) x + O(\log x)$$

$$(6.2) \quad R_{m2}(x) = \alpha_{r-1} \beta_{r-1}(B, C) x^{r-1} + O(x^{r-2}) \quad \text{für } m \geq 5$$

$$(6.3) \quad I_{m2}(x) = \alpha_r x^r - \alpha_{r-1} \beta_{r-1}(B, C) x^{r-1} + O(\psi_r(x)) \quad \text{für } m \geq 4.$$

Zur Formulierung des Hauptsatzes 3 seien noch folgende Festsetzungen getroffen: Es sei

$B(z) = (z - b)^s$; $C^*(z) = C(z + b) = c_1^* z^{s-1} + \dots + c_{s-1}^* z + c$, wobei $c \neq 0$, da $B^*(z) = B(z + b) = z^s$ und $C^*(z)$ teilerfremd sind, ferner $T(c)$ die Anzahl der positiven Teiler von c . Falls $s \geq 2$, sei außerdem für jeden Teiler d von c , wenn noch $\frac{c}{d} = e$ gesetzt ist,

$$D_1(u) = \begin{vmatrix} c_1^* & u & 1 & 0 & \dots & 0 & 0 & 0 \\ c_2^* & d & u & 1 & \dots & 0 & 0 & 0 \\ c_3^* & 0 & d & u & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ c_{s-2}^* & 0 & 0 & 0 & \dots & d & u & 1 \\ c_{s-1}^* & 0 & 0 & 0 & \dots & 0 & d & u \\ e & 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{vmatrix}, \quad D_2(u) = \begin{vmatrix} c_2^* & u & 1 & 0 & \dots & 0 & 0 & 0 \\ c_3^* & d & u & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ c_{s-2}^* & 0 & 0 & 0 & \dots & d & u & 1 \\ c_{s-1}^* & 0 & 0 & 0 & \dots & 0 & d & u \\ e & 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{vmatrix}$$

(im Falle $s = 2$: $D_1(u) = \begin{vmatrix} c_1^* & u \\ e & 1 \end{vmatrix}$, $D_2(u) = e$), sowie $q(d)$ die Anzahl der ganzen Zahlen u , für welche $0 \leq u < |d|^{s-1}$, $D_1(u) \equiv 0 \pmod{d^{s-1}}$ und $D_2(u) \equiv 0 \pmod{d^{s-2}}$.

Schließlich sei gesetzt:

$$(7.1) \quad \beta'_1(b, C) = 4 T(c) (1 + b^2)^{-1/2},$$

$$(7.2) \quad \beta'_s(b, C) = 4 s^{-1} (1 + b^2)^{-1/2} \sum_{d|c} q(d) |d|^{-(s-1)} \quad \text{für } s \geq 2.$$

Dann gilt der

Hauptsatz 3. Die Anzahl der reduziblen bzw. der irreduziblen Polynome $f(z)$ aus $\mathfrak{R}_m(x)$ ist, falls $B(z) = (z - b)^s$ und $s \leq \frac{m+3}{2}$:

$$(8.1) \quad R_{m, m-1}(x) = O(1)$$

$$(8.2) \quad I_{m, m-1}(x) = \alpha_1 x + O(1)$$

$$(8.3) \quad R_{m, m-2}(x) = \alpha_1 \beta_1(B, C) x + O(x^{1/2})$$

$$(8.4) \quad I_{m, m-2}(x) = \alpha_2 x^2 - \alpha_1 \beta_1(B, C) x + O(\psi_2(x))$$

$$(8.5) \quad R_{m, m-3}(x) = \alpha_2 \beta_2(B, C) x^2 + \beta'_{m-3}(b, C) x \log x + O(x)$$

$$(8.6) \quad I_{m, m-3}(x) = \alpha_3 x^3 - \alpha_2 \beta_2(B, C) x^2 - \beta'_{m-3}(b, C) x \log x + O(\psi_3(x))$$

$$(8.7) \quad R_{ms}(x) = \alpha_{r-1} \beta_{r-1}(B, C) x^{r-1} + O(x^{r-2}) \quad \left. \vphantom{R_{ms}(x)} \right\} \quad \text{für}$$

$$(8.8) \quad I_{ms}(x) = \alpha_r x^r - \alpha_{r-1} \beta_{r-1}(B, C) x^{r-1} + O(\psi_r(x)) \quad \left. \vphantom{I_{ms}(x)} \right\} \quad s \leq m - 4.$$

Da bekanntlich $x^{1/2} = O(\psi_2(x))$ und $x^{r-2} = O(\psi_r(x))$ für $r \geq 3$ gilt²⁾, sind alle Restabschätzungen endgültig. Wegen (2) und (3) genügt stets der Nachweis der Gleichungen für die Anzahlen $R_{ms}(x)$. Im folgenden wird durchwegs $x \geq 1$ angenommen. Die Zeichen $\alpha_r, \beta_r(B, C), \beta'_s(b, C)$ bleiben nur den in den Gleichungen (3), (4) und (7) erklärten Konstanten vorbehalten. Mit $\gamma, \gamma', \gamma'', \gamma_1, \dots, \gamma_{24}$ werden gewisse, nicht näher interessierende, allein von $m, s, B(z)$ und $C(z)$ abhängige positive Konstanten bezeichnet.

I.

Ist $f(z)$ reduzibel, so gibt es zwei ganzzahlige Polynome

$$f_1(z) = z^k + u_1 z^{k-1} + \dots + u_k$$

und

$$f_2(z) = z^l + v_1 z^{l-1} + \dots + v^l$$

mit $1 \leq k \leq l \leq m - 1$ und $k + l = m$, so daß $f(z) = f_1(z) f_2(z)$. $\mathfrak{P}_{mrk}$ bezeichne stets die Menge der (im Falle $k = l$ geordneten) Paare $f_1(z), f_2(z)$, für die mit einem geeigneten Polynom $g(z)$ die Gleichung

$$(9) \quad f_1(z) f_2(z) = B(z) g(z) + C(z)$$

erfüllt ist. $\mathfrak{P}_{mrk}(x)$ sei die Menge, $P_{mrk}(x)$ die Anzahl der Paare aus $\mathfrak{P}_{mrk}$, deren zugehöriges Polynom $g(z)$ die Normbedingung (N) erfüllt. Nach (9) sind sowohl $f_1(z)$ und $B(z)$ als auch $f_2(z)$ und $B(z)$ teilerfremd; denn $B(z)$ und $C(z)$ sind teilerfremd nach Voraussetzung.

²⁾ Dies folgt unmittelbar aus den Gleichungen (7.1) bis (7.4) in ZPII und der dort angeführten Literatur.

Für spätere Abschätzungen benötigen wir oft den

Satz 1. Jedes Paar $f_1(z), f_2(z)$ aus $\mathfrak{P}_{m\tau k}(x)$ erfüllt die Ungleichung

$$(N') \quad 1 \leq N(f_1) N(f_2) \leq \gamma N(g) \leq \gamma x.$$

Beweis. Aus Satz 1 in ZPIV, der Dreiecksungleichung und (N) folgt:
 $1 \leq N(f_1) N(f_2) \leq \gamma_1 N(f_1 f_2) = \gamma_1 N(Bg + C) \leq \gamma_1 N(Bg) + \gamma_1 N(C)$
 $\leq \gamma_2 N(B) N(g) + \gamma_3 \leq \gamma N(g) \leq \gamma x.$

Zur Vereinfachung der Schreibweise sollen durchweg folgende Bezeichnungen gelten:

$$(10) \quad \begin{aligned} b_0 &= t_0 = u_0 = v_0 = 1; \quad b_\sigma = 0 \quad \text{für } \sigma \leq -1 \text{ und } \sigma \geq s+1; \\ c_\sigma &= 0 \quad \text{für } \sigma \leq 0 \text{ und } \sigma \geq s+1; \quad t_\varrho = 0 \quad \text{für } \varrho \leq -1 \text{ und } \varrho \geq r+1; \\ u_\kappa &= 0 \quad \text{für } \kappa \leq -1 \text{ und } \kappa \geq k+1; \quad v_\lambda = 0 \quad \text{für } \lambda \leq -1 \text{ und } \lambda \geq l+1. \end{aligned}$$

Die Gleichung (9) ist folgendem Gleichungssystem äquivalent:

$$(11) \quad \sum_{\lambda=0}^l u_{\mu-\lambda} v_\lambda = c_{\mu-r} + \sum_{\varrho=0}^r b_{\mu-\varrho} t_\varrho (= a_\mu) \quad \text{für } 0 \leq \mu \leq m.$$

$\mathfrak{P}_{m\tau k}$ ist daher die Menge aller Paare $f_1(z), f_2(z)$, für welche das System (11) ganzzahlige Lösungen $u_1, \dots, u_k, v_1, \dots, v_l, t_1, \dots, t_r$ hat. Man kann (11) als lineares Gleichungssystem von m Gleichungen für die $l+r$ Unbekannten $v_\lambda, 1 \leq \lambda \leq l$, und $t_\varrho, 1 \leq \varrho \leq r$, auffassen. Die Größenbeziehung zwischen $l+r$ und m , also zwischen r und k , ist daher für die Lösungsanzahl von großer Bedeutung.

Ist $f_1(z)$ fest vorgegeben, betrachten wir zunächst die Polynome

$$f'_2(z) = v'_1 z^{s-1} + \dots + v'_s \quad \text{und} \quad g'(z) = t'_1 z^{k-1} + \dots + t'_k,$$

die der Gleichung

$$(12.1) \quad f_1(z) f'_2(z) = B(z) g'(z) + C(z),$$

also dem Gleichungssystem

$$(12.2) \quad \sum_{\sigma=1}^s u_{\mu-\sigma} v'_\sigma + \sum_{\kappa=1}^k b_{\mu-\kappa} (-t'_\kappa) = c_{\mu-k}, \quad 1 \leq \mu \leq s+k$$

mit $s+k$ Gleichungen für $s+k$ Unbekannte genügen, dessen Determinante die nicht verschwindende Resultante der teilerfremden Polynome $f_1(z)$ und $B(z)$ ist. Durch $f_1(z)$ sind $f'_2(z)$ und $g'(z)$ eindeutig bestimmt, allerdings nicht immer ganzzahlig. Für jedes $k \geq 1$ bezeichne $\mathfrak{M}_k$ die Menge der Polynome $f_1(z)$, für welche $f'_2(z)$ und daher wegen (12.2) auch $g'(z)$ ganzzahlig ist.

Wir beweisen nun den

Satz 2. Ist $k \leq r$, so ist $\mathfrak{P}_{m\tau k}$ gleich der Menge aller Paare $f_1(z), f_2(z)$ normierter ganzzahliger Polynome der Grade k und l mit $1 \leq k \leq l \leq m-1$ und $k+l=m$, für welche die Bedingungen gelten:

$$(13) \quad f_1(z) \in \mathfrak{M}_k \quad \text{und} \quad f_2(z) \equiv f'_2(z) \pmod{B(z)}.$$

Ist $k = r$ oder sind die Koeffizienten $t_1, \dots, t_{r-k}$ des zugehörigen Polynoms $g(z)$ vorgegeben, so ist $f_2(z)$ durch $f_1(z)$ eindeutig bestimmt.

Beweis. Jedes Paar $f_1(z), f_2(z)$, welches die Bedingungen (13) erfüllt, gehört zu $\mathfrak{P}_{mrk}$; dies folgt wegen (12.1) aus

$$f_1(z) f_2(z) \equiv f_1(z) f_2'(z) \equiv C(z) \pmod{B(z)}.$$

Ist $f_1(z), f_2(z)$ ein beliebiges Paar aus $\mathfrak{P}_{mrk}$, so gibt es wegen $l \geq s$ ein eindeutig bestimmtes, ganzzahliges Polynom $f_2''(z)$, dessen Grad höchstens $s - 1$ ist, so daß $f_2(z) \equiv f_2''(z) \pmod{B(z)}$, also $f_1(z) f_2''(z) \equiv C(z) \pmod{B(z)}$. Da $f_2'(z)$ und $f_2''(z)$ eindeutig bestimmt sind, sind sie identisch und $f_1(z)$ gehört zu $\mathfrak{M}_k$. Setzt man

$$(14.1) \quad \bar{f}_2(z) = f_2(z) - f_2'(z) \quad \text{und} \quad \bar{g}(z) = g(z) - g'(z),$$

so erhält man aus (9), (12.1) und (13):

$$f_1(z) \bar{f}_2(z) = B(z) \bar{g}(z)$$

sowie

$$(14.2, 3) \quad \bar{f}_2(z) = B(z) h(z) \quad \text{und} \quad \bar{g}(z) = h(z) f_1(z).$$

Hierbei ist $h(z) = z^{r-k} + w_1 z^{r-k-1} + \dots + w_{r-k}$ mit ganzzahligen w_i .

Die Polynome $\bar{f}_2(z)$ und $\bar{g}(z)$ haben die Grade l bzw. r und stimmen mit $f_2(z)$ bzw. $g(z)$ wegen $r - k = l - s$ außer im Anfangskoeffizienten 1 noch in den folgenden $r - k$ Koeffizienten $v_1, \dots, v_{r-k}$ bzw. $t_1, \dots, t_{r-k}$ überein. Aus (14.3) folgt daher

$$(14.4) \quad \begin{array}{rcl} u_1 + & w_1 & = t_1 \\ u_2 + & u_1 w_1 + w_2 & = t_2 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ u_{r-k} + u_{r-k+1} w_1 + \dots + w_{r-k} & = & t_{r-k}. \end{array}$$

Bei gegebenem $f_1(z)$ ist somit $h(z)$ durch $t_1, \dots, t_{r-k}$ eindeutig bestimmt, also wegen (14.2) auch

$$f_2(z) = B(z) h(z) + f_2'(z).$$

Für Abschätzungen benötigen wir mehrmals den

Satz 3. Ist $k \leq r$, so ist

$$P_{mrk}(x) = O\left(x^{r-k} \sum_{\substack{1 \leq N(f_1) \leq \gamma x \\ f_1 \in \mathfrak{M}_k}} N(f_1)^{-(r-k)}\right).$$

Hierbei wird über alle Polynome $f_1(z)$ aus $\mathfrak{M}_k$ summiert, welche die Bedingung $1 \leq N(f_1) \leq \gamma x$ erfüllen.

Beweis. Zu fest gewähltem $f_1(z)$ aus $\mathfrak{M}_k$ gibt es nach Satz 2 bei vorgegebenen $t_1, \dots, t_{r-k}$ genau ein Paar $f_1(z), f_2(z)$ aus $\mathfrak{P}_{mrk}$. Nach Satz 1

und wegen $N(f_2) \geq (1 + v_1^2 + \dots + v_{r-k}^2)^{1/2}$ erfüllt jedes Paar $f_1(z), f_2(z)$ aus $\mathfrak{P}_{m\tau k}(x)$ die Bedingung

$$1 \leq N(f_1) (1 + v_1^2 + \dots + v_{r-k}^2)^{1/2} \leq \gamma x.$$

Diese ist äquivalent den Bedingungen

$$(N'') \quad 1 \leq N(f_1) \leq y \quad \text{und} \quad 1 + v_1^2 + \dots + v_{r-k}^2 \leq \left(\frac{y}{N(f_1)}\right)^2 \quad \text{mit} \quad y = \gamma x.$$

Ist $Q_{m\tau k}(y)$ die Anzahl der Paare $f_1(z), f_2(z)$ aus $\mathfrak{P}_{m\tau k}$, die den Bedingungen (N'') genügen, so ist wegen $P_{m\tau k}(x) \leq Q_{m\tau k}(y)$ nur zu zeigen

$$(15) \quad Q_{m\tau k}(y) = O\left(y^{r-k} \sum_{\substack{1 \leq N(f_1) \leq y \\ f_1 \in \mathfrak{M}_k}} N(f_1)^{-(r-k)}\right).$$

Aus (14.4) ergibt sich

$$w_i = \sum_{\varrho=0}^{r-k} w_{\varrho i}(u) t_{\varrho}, \quad 0 \leq i \leq r-k,$$

wobei die $w_{\varrho i}(u)$ ganzzahlige Polynome in $u_1, \dots, u_k$ sind. Aus (14.2) folgt, da $f_2(z)$ die Koeffizienten $1, v_1, \dots, v_{r-k}$ hat:

$$v_{\lambda} = \sum_{i=0}^{\lambda} b_{\lambda-i} w_i = \sum_{i=0}^{\lambda} \sum_{\varrho=0}^{r-k} b_{\lambda-i} w_{\varrho i}(u) t_{\varrho} = \sum_{\varrho=0}^{r-k} v_{\lambda \varrho}(u) t_{\varrho}, \quad 0 \leq \lambda \leq r-k,$$

wobei die $v_{\lambda \varrho}(u)$ ganzzahlige Polynome in $u_1, \dots, u_k$ sind, deren Koeffizienten nur von $B(z)$ abhängen. Die zweite Bedingung von (N'') geht über in

$$1 + v_1^2 + \dots + v_{r-k}^2 = \sum_{i,j=0}^{r-k} V_{ij}(u) t_i t_j \leq \left(\frac{y}{N(f_1)}\right)^2,$$

wobei die $V_{ij}(u)$ eine positiv-definite Matrix bilden. Die Anzahl der Polynome $f_2(z)$, die diese Bedingung bei festem $f_1(z)$ erfüllen, ist daher gleich der Anzahl der Gitterpunkte $t_1, \dots, t_{r-k}$ im Innern und auf dem Rande des entsprechenden $r-k$ -dimensionalen Ellipsoids, also bekanntlich ein $O\left(V_0(u)^{-1/2} \left(\frac{y}{N(f_1)}\right)^{r-k}\right)$, wenn $V_0(u)$ die zu $V_{00}(u)$ gehörige Unterdeterminante der Matrix $\|V_{ij}(u)\|$ bedeutet. Da die $v_{\lambda \varrho}(u)$ und somit auch die $V_{ij}(u)$ ganzzahlig sind, ist $V_0(u) \geq 1$. Hieraus folgt sofort (15) und die Behauptung.

Ist $f'_1(z) = u'_1 z^{s-1} + \dots + u'_s$ ein ganzzahliges, zu $B(z)$ teilerfremdes Polynom, dessen Grad höchstens gleich $s-1$ ist, so gibt es ein eindeutig bestimmtes Polynom $f'_2(z)$ vom Grade kleiner oder gleich $s-1$ derart, daß $f'_1(z) f'_2(z) \equiv C(z) \pmod{B(z)}$. Denn das aus

$$(16) \quad f'_1(z) f'_2(z) = B(z) g''(z) + C(z)$$

hervorgehende lineare Gleichungssystem für die Koeffizienten von $f'_2(z)$ und $g''(z)$ hat je $2s-1$ Unbekannte und Gleichungen und die Resultante $R(f'_1, B) \neq 0$ als Determinante.

$\mathfrak{M}'_s$ sei die Menge aller Polynome $f'_1(z)$, für welche auch $f'_2(z)$ ganzzahlig ist. Dann gilt der

Satz 4. Ist $s \leq k$, so ist $\mathfrak{M}_k$ gleich der Menge aller normierten Polynome vom Grade k , welche die Kongruenz

$$f_1(z) \equiv f'_1(z) \pmod{B(z)}, \quad f'_1(z) \in \mathfrak{M}'_s$$

erfüllen.

Beweis. Ist $f_1(z)$ aus $\mathfrak{M}_k$ und $k \geq s$, dann gibt es ein ganzzahliges Polynom $f'_1(z)$ vom Grade kleiner oder gleich $s - 1$, so daß $f_1(z) \equiv f'_1(z) \pmod{B(z)}$. Dann ist auch $f'_1(z) f'_2(z) \equiv C(z) \pmod{B(z)}$, d. h. $f'_1(z)$ aus $\mathfrak{M}'_s$. Umgekehrt folgt $f_1(z) f'_2(z) \equiv C(z) \pmod{B(z)}$ aus $f_1(z) \equiv f'_1(z) \pmod{B(z)}$ und $f'_1(z) f'_2(z) \equiv C(z) \pmod{B(z)}$.

Aus den beiden letzten Sätzen folgt der

Satz 5. Ist $s \leq k$, so ist

$$P_{mrk}(x) = O(x^{r-s} \sum_{\substack{1 \leq N(f'_1) \leq \gamma' x \\ f'_1 \in \mathfrak{M}'_s}} N(f'_1)^{-(r-k)})$$

Beweis. Es ist $s \leq k \leq l \leq r$. $\mathfrak{M}_k$ ist nach Satz 4 die Menge aller Polynome $f_1(z) = B(z) h_1(z) + f'_1(z)$, wobei $f'_1(z)$ zu $\mathfrak{M}'_s$ gehört und $h_1(z)$ ein beliebiges normiertes Polynom vom Grad $k - s$ ist.

$N(f_1)^2 = N(f'_1 + h_1 B)^2$ ist eine positiv-definite quadratische Form der Koeffizienten von $f'_1(z)$ und $h_1(z)$. Daher ist

$$N(f_1)^2 \geq \gamma_4^2 (N(h_1)^2 + N(f'_1)^2).$$

Wegen $r - k \geq 0$ ergibt sich dann

$$\begin{aligned} \sum_{\substack{1 \leq N(f_1) \leq \gamma' x \\ f_1 \in \mathfrak{M}_k}} N(f_1)^{-(r-k)} &\leq \sum_{\substack{1 \leq N(h_1)^2 + N(f'_1)^2 \leq \gamma^2 \gamma_4^{-2} x^2 \\ f'_1 \in \mathfrak{M}'_s}} \gamma_5 (N(h_1)^2 + N(f'_1)^2)^{-\frac{r-k}{2}} \\ &\leq \sum_{1 \leq (h_1) \leq \gamma' x} \sum_{\substack{1 \leq N(f'_1) \leq \gamma' x \\ f'_1 \in \mathfrak{M}'_s}} \gamma_5 N(f'_1)^{-(r-k)} \leq \gamma_6 x^{k-s} \sum_{\substack{1 \leq N(f'_1) \leq \gamma' x \\ f'_1 \in \mathfrak{M}'_s}} N(f'_1)^{-(r-k)} \end{aligned}$$

und aus Satz 3 die Behauptung.

Im Falle $k > r$ gilt der

Satz 6. Ist $k \geq r + 1$, so ist $\mathfrak{P}_{mrk}$ gleich der Menge aller Paare $f_1(z), f'_2(z)$, für welche $f_1(z)$ zu $\mathfrak{M}_k$ gehört und $f'_2(z)$ den (genauen) Grad l hat und normiert ist, d. h. die Gleichungen bestehen:

$$v'_\sigma = 0 \quad \text{für} \quad 1 \leq \sigma \leq k - r - 1 \quad \text{und} \quad v'_{k-r} = 1.$$

Beweis. Ist $k \geq r + 1$, also $l \leq s - 1$, so kann bei gegebenem $f_1(z)$ die Gleichung (9) nur dann bestehen, wenn $f_2(z) = f'_2(z)$ und $g(z) = g'(z)$; denn $f_2(z)$ und $g'(z)$ sind durch $f_1(z)$ eindeutig bestimmt. $f_2(z)$ hat aber den Grad l und ist normiert.

II.

Wir wenden uns nun denjenigen Fällen zu, bei welchen zur Bestimmung bzw. Abschätzung der Anzahlen $P_{mrk}(x)$ keine Unterscheidung bezüglich der Eigenschaften von $B(z)$ notwendig ist.

Satz 7. Für $2 \leq k \leq r-2$, $r \geq 5$ und beliebiges m ist:

$$P_{mrk}(x) = O(x^{r-2}).$$

Beweis. Wir wenden den Satz 3 unter Verzicht auf die Bedingung $f_1(z) \in \mathfrak{M}_k$ an. Nach bekannter Methode ergibt sich:

$$\begin{aligned} P_{mrk}(x) &= O \left(x^{r-k} \sum_{1 \leq 1+u_1^2+\dots+u_k^2 \leq (\gamma x)^2} (1+u_1^2+\dots+u_k^2)^{-\frac{r-k}{2}} \right) \\ &= O \left(x^{r-k} \int_1^{\gamma x} (1+u^2)^{-\frac{r-k}{2}} u^{k-1} du \right) = O \left(x^{r-k} \int_1^{\gamma x} u^{2k-r-1} du \right) \end{aligned}$$

und hieraus die Behauptung.

Wir betrachten nun den Fall $k=1$ und setzen $f_1(z) = z - u$. Ein Paar $z - u, f_2(z)$ gehört bekanntlich genau dann zu $\mathfrak{P}_{mr1}$, wenn $f(z) = (z - u) f_2(z)$ die Bedingung $f(u) = 0$, also

$$(17) \quad B(u)g(u) + C(u) = 0$$

erfüllt. Da $B(z)$ und $C(z)$ teilerfremd sind, können $B(u)$ und $C(u)$ nie gleichzeitig verschwinden. Wegen (17) ist für alle Paare aus $\mathfrak{P}_{mr1}$ $B(u) \neq 0$ und $\frac{C(u)}{B(u)}$ ganzzahlig. Die wegen $\lim_{z \rightarrow \pm \infty} \frac{C(z)}{B(z)} = 0$ endliche Menge aller ganzen

Zahlen u , welche diesen beiden Bedingungen genügen, sei $\mathfrak{T}(B, C)$.

Ist $P_{mr1}(x, u)$ die Anzahl der Paare $z - u, f_2(z)$ aus $\mathfrak{P}_{mr1}(x)$, für welche u eine feste Zahl aus $\mathfrak{T}(B, C)$ ist, so gilt der

Satz 8. Für $r \geq 2$ ist

$$P_{mr1}(x, u) = \alpha_{r-1} (1 + u^2 + \dots + u^{2r-2})^{-1/2} x^{r-1} + O(x^{r-2}).$$

Beweis. Für jedes Paar $z - u, f_2(z)$ aus $\mathfrak{P}_{mr1}$ folgt aus (17) die Gleichung

$$(18) \quad -t_r = d + u^r + u^{r-1}t_1 + \dots + ut_{r-1} \quad \text{mit} \quad d = \frac{C(u)}{B(u)}.$$

Setzt man t_r aus (18) in die Normbedingung (N) ein, so erhält man die Ungleichung

$$(19) \quad \sum_{i,j=0}^{r-1} g_{ij} t_i t_j \leq x^2,$$

wobei außer $t_0 = 1$ gesetzt ist:

$$\begin{aligned} g_{00} &= (d + u^r)^2, \quad g_{0i} = g_{i0} = (d + u^r) u^{r-i} \quad \text{für} \quad 1 \leq i \leq r-1, \\ g_{ii} &= 1 + u^{2r-2i} \quad \text{für} \quad 1 \leq i \leq r-1 \quad \text{sowie} \quad g_{ij} = u^{2r-i-j} \quad \text{für} \quad 1 \leq i, j \leq r-1 \end{aligned}$$

und $i \neq j$. $P_{m\tau 1}(x, u)$ ist daher gleich der Anzahl der Gitterpunkte $t_1, \dots, t_{r-1}$ im Innern und auf dem Rande des durch die Ungleichung (19) dargestellten $r-1$ -dimensionalen Ellipsoids. Durch Transformation auf Mittelpunktskoordinaten $z_1, \dots, z_{r-1}$ ergibt sich aus (19) die Bedingung

$$\sum_{i,j=1}^{r-1} g_{ij} z_i z_j \leq x^2 - \frac{G(u)}{G_0(u)} \quad \text{mit} \quad z_i = t_i + \frac{G_i(u)}{G_0(u)}, \quad 1 \leq i \leq r-1,$$

wobei $G(u)$ die Determinante der Matrix $\|g_{ij}\|$ und $G_i(u)$ für $0 \leq i \leq r-1$ jeweils die zu g_{0i} gehörige Unterdeterminante bedeutet. Hieraus folgt:

$$\begin{aligned} P_{m\tau 1}(x, u) &= \alpha_{r-1} G_0(u)^{-1/2} \left(x^2 - \frac{G(u)}{G_0(u)} \right)^{\frac{r-1}{2}} + O(x^{r-2}) \\ &= \alpha_{r-1} G_0(u)^{-1/2} x^{r-1} + O(x^{r-2}) \end{aligned}$$

und die Behauptung aus

$$\begin{aligned} G_0(u) &= \begin{vmatrix} 1 + u^{2r-2} & u^{2r-3} & \dots & u^{r+1} & u^r \\ u^{2r-3} & 1 + u^{2r-4} & \dots & u^r & u^{r-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ u^{r+1} & u^r & \dots & 1 + u^4 & u^3 \\ u^r & u^{r-1} & \dots & u^3 & 1 + u^2 \end{vmatrix} \\ &= \begin{vmatrix} 1 & 0 & \dots & 0 & u^r \\ 0 & 1 & \dots & 0 & u^{r-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & u^3 \\ -u^{r-2} & -u^{r-3} & \dots & -u & 1 + u^2 \end{vmatrix} \\ &= 1 + u^2 + \dots + u^{2r-2}. \end{aligned}$$

Satz 9. $P_{m11}(x) = O(1)$

$$P_{m\tau 1}(x) = \alpha_{r-1} \beta_{r-1}(B, C) x^{r-1} + O(x^{r-2}) \quad \text{für } r \geq 2.$$

Beweis. Für $r = 1$ geht die Gleichung (18) über in

$$-t_1 = u + \frac{C(u)}{B(u)}.$$

Zu jedem $u \in \mathfrak{T}(B, C)$ gibt es genau je ein Polynom $g(z)$ und $f_2(z)$, also besteht $\mathfrak{P}_{m11}$ aus höchstens endlich vielen Paaren $z = u, f_2(z)$.

Für $r \geq 2$ gilt

$$P_{m\tau 1}(x) = \sum_{u \in \mathfrak{T}(B, C)} P_{m\tau 1}(x, u),$$

und die Behauptung ergibt sich aus Satz 8 und Gleichung (4).

$\mathfrak{P}_{m\tau}(x)$ sei die Menge, $P_{m\tau}(x)$ die Anzahl der Tripel $z = u, z = v, f_3(z)$ mit $u \neq v$ und folgenden Eigenschaften:

Es ist $f(z) = (z - u)(z - v)f_3(z) \equiv C(z) \pmod{B(z)}$; das zu $f(z)$ gehörige Polynom $g(z)$ erfüllt die Bedingung (N). Dann gilt der

Satz 10. $P_{m_r}(x) = O(x^{r-2})$ für $r \geq 2$.

Beweis. Alle Tripel aus $\mathfrak{P}_{m_r}(x)$ genügen folgenden Bedingungen:

$$B(u)g(u) + C(u) = 0; \quad B(v)g(v) + C(v) = 0; \quad u, v \in \mathfrak{T}(B, C).$$

Hieraus folgt:

$$u^r + t_1 u^{r-1} + \cdots + t_{r-1} u + t_r + d_1 = 0 \quad \text{mit} \quad d_1 = \frac{C(u)}{B(u)},$$

$$v^r + t_1 v^{r-1} + \cdots + t_{r-1} v + t_r + d_2 = 0 \quad \text{mit} \quad d_2 = \frac{C(v)}{B(v)}.$$

Bei vorgegebenen $t_1, \dots, t_{r-2}$ hat die Determinante des Gleichungssystems den Wert $u - v \neq 0$. Dann sind t_{r-1} und t_r eindeutig bestimmt, jedoch nicht immer ganzzahlig.

Ist $r = 2$, so gibt es zu jedem der (endlich vielen) Paare u, v höchstens ein Paar ganzzahliger t_1, t_2 , also höchstens endlich viele Polynome $g(z)$ und $f_3(z)$.

Im Falle $r \geq 3$ ist wegen $N(g)^2 \geq t_1^2 + \cdots + t_{r-2}^2$ die Anzahl der Tripel aus $\mathfrak{P}_{m_r}(x)$ mit festem u und v höchstens so groß wie die Anzahl der $r - 2$ -tupel $t_1, \dots, t_{r-2}$, welche die Ungleichung $t_1^2 + \cdots + t_{r-2}^2 \leq x^2$ erfüllen, also ein $O(x^{r-2})$.

Der Hauptsatz 1 ergibt sich jetzt, abgesehen vom Fall $m = 5, s = 1$, folgendermaßen: Jedes Polynom $f(z)$ aus $\mathfrak{H}_{m_s}(x)$ wird in mindestens einer der Paarmengen $\mathfrak{P}_{m_r k}(x)$, $1 \leq k \leq \left[\frac{m}{2} \right]$, mitgezählt, einige sogar mehrfach. Im Falle $k = 1$ werden nur diejenigen Polynome $f(z)$ mehrfach gezählt, welche auch in der Menge $\mathfrak{P}_{m_r}(x)$ enthalten sind. Daher ist

$$(20) \quad R_{m_s}(x) = P_{m_r 1}(x) + O(P_{m_r}(x)) + \sum_{k=2}^{\left[\frac{m}{2} \right]} O(P_{m_r k}(x)).$$

Die Gleichungen (5.1), (5.3) und (5.5) folgen sofort aus den Sätzen 9 und 10. Die Gleichung (5.7) folgt für $m \geq 6$ wegen $r = m - s \geq \frac{m+3}{2}$, also $\left[\frac{m}{2} \right] \leq r - 2$ und $r \geq 5$, aus den Sätzen 9, 10 und 7. Für den noch verbleibenden Fall $m = 5, s = 1$ wird die Gleichung (5.7) am Schluß des Abschnitts IV bewiesen.

III.

Dieser Abschnitt ist dem Fall gewidmet, daß $s = 2$ und die Diskriminante $\Delta = b_1^2 - 4b_2$ des Polynoms $B(z) = z^2 + b_1 z + b_2$ nicht verschwindet. Dann gilt zunächst der

Satz 11. Ist $B(z) = z^2 + b_1 z + b_2$ mit $\Delta = b_1^2 - 4 b_2 \neq 0$, so gilt für jedes $d \neq 0$:

$$\sum_{u^2 - b_1 u v + b_2 v^2 = d} (u^2 + v^2)^{-1/2} = O(1) \quad \text{und} \quad \sum_{\substack{u^2 - b_1 u v + b_2 v^2 = d \\ u^2 + v^2 \leq x^2}} 1 = O(\log x).$$

Beweis. Ist Δ eine Quadratzahl $\neq 0$ oder ist $\Delta < 0$, so hat die Gleichung $u^2 - b_1 u v + b_2 v^2 = d$ bekanntlich höchstens endlich viele ganzzahlige Lösungen. Es bleibt also nur der Fall, daß $\Delta > 0$ und keine Quadratzahl ist.

Die Lösungen u, v der Gleichung $u^2 - b_1 u v + b_2 v^2 = d$ kann man eindeutig den Lösungen w, v , der Gleichung

$$(21) \quad w^2 - D v^2 = d'$$

zuordnen, und zwar mit Hilfe der Beziehungen

$$u - \frac{b_1}{2} v = w, \quad D = \frac{\Delta}{4}, \quad d = d', \quad \text{falls } b_1 \equiv 0 \pmod{2},$$

bzw.

$$2 u - b_1 v = w, \quad D = \Delta, \quad d' = 4 d, \quad \text{falls } b_1 \not\equiv 0 \pmod{2}.$$

Wie man leicht sieht, ist D stets ganzzahlig, während die Ganzzahligkeit von w und v aus der von u und v folgt und umgekehrt. Weiter gilt

$$u^2 + v^2 \geq \gamma_7 (w^2 + v^2);$$

denn

$$u^2 + v^2 = \left(w + \frac{b_1}{2} v\right)^2 + v^2 \quad \text{bzw.} \quad u^2 + v^2 = \left(\frac{w}{2} + \frac{b_1}{2} v\right)^2 + v^2$$

sind positiv-definite quadratische Formen in u und v . Außerdem sind mit jedem Paar w, v auch die Paare $w, -v$; $-w, v$ und $-w, -v$ Lösungen der Gleichung (21), während es nur höchstens zwei Lösungen mit $w = 0$ bzw. $v = 0$ gibt. Es genügt daher zu zeigen:

$$(22) \quad \sum_{\substack{w^2 - D v^2 = d' \\ w, v > 0}} (w^2 + v^2)^{-1/2} = O(1) \quad \text{und} \quad \sum_{\substack{w^2 - D v^2 = d' \\ w^2 + v^2 \leq \gamma_8 x^2 \\ w, v > 0}} 1 = O(\log x).$$

Falls überhaupt Lösungen der Gleichung (21) existieren, lassen sie sich bekanntlich in eine endliche Anzahl von Klassen einteilen. Die Lösungen jeder Klasse mit $w > 0$ und $v > 0$ lassen sich so in zwei Folgen $w_0, w_1, \dots$ und $v_0, v_1, \dots$ anordnen, daß gilt³⁾:

$$w_n + \sqrt{D} v_n = (w_0 + \sqrt{D} v_0) (W + \sqrt{D} V)^n, \quad n = 0, 1, 2, \dots,$$

wobei W und V gewisse positive ganze Zahlen sind, welche die Gleichung

$$W^2 - D V^2 = 1$$

³⁾ Vgl. etwa E. LANDAU, Vorlesungen über Zahlentheorie, Bd. I, I. Teil, Kap. 7 und IV. Teil, Kap. 4, Sätze 201—203 einschließlich der Zwischenbemerkungen und Beweise.

erfüllen. Hieraus folgt für jedes $n \geq 1$, da alle auftretenden Größen positiv sind:

$$\begin{aligned} w_n &= W w_{n-1} + D V_{n-1}; \quad v_n = V w_{n-1} + W v_{n-1}; \\ w_n^2 + v_n^2 &> (W^2 + V^2) w_{n-1}^2 + (D^2 V^2 + W^2) v_{n-1}^2 > (D+1) (w_{n-1}^2 + v_{n-1}^2); \\ w_n^2 + v_n^2 &> (D+1)^n (w_0^2 + v_0^2) > (D+1)^n. \end{aligned}$$

Die Reihe $\sum_{n=1}^{\infty} (w_n^2 + v_n^2)^{-1/2}$ ist daher konvergent und es gilt

$$\sum_{\substack{w_n^2 + v_n^2 \leq \gamma_8 x^2 \\ n \geq 0}} 1 \leq \sum_{\substack{(D+1)^n \leq \gamma_8 x^2 \\ n \geq 0}} 1 = 1 + \left[\frac{\log \gamma_8 x^2}{\log (D+1)} \right] = O(\log x).$$

Da nur endlich viele Lösungsklassen der Gleichung (21) möglich sind, ergeben sich hieraus sofort die Gleichungen (22).

Satz 12. Falls $B(z) = z^2 + b_1 z + b_2$ und $\Delta = b_1^2 - 4b_2 \neq 0$, ist

$$P_{mrk}(x) = O(x^{r-2}) \text{ für } 2 \leq k \leq \left[\frac{m}{2} \right] \text{ und } r \geq 3,$$

$$P_{422}(x) = O(\log x).$$

Beweis. Wegen $s = 2$ und $k \geq 2$ brauchen wir nach Satz 5 nur zu zeigen:

$$(23.1) \quad \sum_{\substack{1 \leq N(f'_1) \leq \gamma' x \\ f'_1 \in \mathfrak{M}'_2}} N(f'_1)^{-(r-k)} = O(1) \quad \text{für } r \geq 3 \quad \text{und}$$

$$(23.2) \quad \sum_{\substack{1 \leq N(f'_1) \leq \gamma' x \\ f'_1 \in \mathfrak{M}'_2}} 1 = O(\log x).$$

Wegen $s - 1 = 1$ setzen wir $f'_1(z) = vz + u$. Aus (16) und bekannten Sätzen über die Resultanten folgt:

$$R(f'_1, B) R(f'_2, B) = R(f'_1 f'_2, B) = R(Bg'' + C, B) = R(C, B).^4)$$

Für jedes Polynom $f'_1(z)$ aus $\mathfrak{M}'_2$ gilt daher

$$R(f'_1, B) = u^2 - b_1 uv + b_2 v^2 \mid R(C, B).$$

$R(C, B)$ ist eine ganze Zahl $\neq 0$ und es ist

$$(24) \quad \sum_{\substack{1 \leq N(f') \leq \gamma' x \\ f'_1 \in \mathfrak{M}'_2}} N(f'_1)^{-(r-k)} \leq \sum_{d \mid R(C, B)} \sum_{\substack{u^2 - b_1 uv + b_2 v^2 = d \\ u^2 + v^2 \leq (\gamma' x)^2}} (u^2 + v^2)^{-\frac{r-k}{2}}.$$

Da für $r \geq 3$ gilt: $k \leq \left[\frac{2}{m} \right] = \left[\frac{r}{2} \right] + 1$, also $r - k \geq 1$, folgen die Gleichungen (23) aus (24) und Satz 11.

Hauptsatz 2 ergibt sich nun aus (20) und den Sätzen 9, 10 und 12.

⁴⁾ Vgl. O. PERRON, Algebra, Bd. I, S. 220 ff. Die Gleichheit der ersten beiden Ausdrücke folgt sofort aus Satz 118, die der beiden letzten läßt sich völlig analog zum Beweis des Satzes 117 zeigen, obwohl dieser etwas von unserem Falle abweichende Voraussetzungen hat.

IV.

Dieser und die folgenden Abschnitte behandeln den Fall $B(z) = (z - b)^s$. Hier ist es meist zweckmäßig, die Transformation $\zeta = z - b$ auszuführen. Für zwei Polynome $B(z)$ und $C(z)$ sollen $\mathfrak{P}_{m\tau k}$, $\mathfrak{P}_{m\tau k}(x)$ und $P_{m\tau k}(x)$ die bisherige Bedeutung haben. Für ein ganzzahliges b sei

$$B^*(z) = B(z + b), \quad C^*(z) = C(z + b),$$

ferner $\mathfrak{P}_{m\tau k}^*$ die Menge der Paare normierter, ganzzahliger Polynome $f_1(z)$, $f_2(z)$ der Grade k und l mit $1 \leq k \leq l \leq m - 1$ und $k + l = m$, für welche mit einem geeigneten Polynom $g(z)$

$$(25.1) \quad f_1(z)f_2(z) = B^*(z)g(z) + C^*(z).$$

Weiter sei gesetzt:

$$(25.2) \quad b_{\varrho i} = \binom{r-i}{\varrho-i} (-b)^{\varrho-i}, \quad 0 \leq i, \varrho \leq r.$$

$\mathfrak{P}_{m\tau k}^*$ bzw. $\mathfrak{P}_{m\tau k}^{**}(x)$ seien die Mengen, $P_{m\tau k}^*(x)$ bzw. $P_{m\tau k}^{**}(x)$ die Anzahlen der Paare $f_1(z)$, $f_2(z)$ aus $\mathfrak{P}_{m\tau k}^*$, für welche das zugehörige Polynom $g(z)$ der Bedingung

$$(N) \quad N(g) \leq x \quad \text{bzw.} \quad (N^{**}) \quad \sum_{\varrho=0}^r \left(\sum_{i=0}^r b_{\varrho i} t_i \right)^2 \leq x^2$$

genügt. Dann gilt der

Satz 13. (1) $P_{m\tau k}^{**}(x) = P_{m\tau k}(x)$.

(2) Für jedes Paar $f_1(z)$, $f_2(z)$ aus $\mathfrak{P}_{m\tau k}^{**}(x)$ gilt $1 \leq N(f_1)N(f_2) \leq \gamma''x$.

(3) Gilt die Abschätzung $P_{m\tau k}(x) = O(\psi(x))$, so gilt auch

$$P_{m\tau k}^*(x) = O(\psi(x)^5).$$

Folgerung: Bei jeder Abschätzung der Anzahlen $P_{m\tau k}(x)$ können wir uns daher auf den Fall $B(z) = z^s$ beschränken.

Dann erhalten die letzten s Gleichungen von (11) die Gestalt:

$$(26) \quad \sum_{\lambda=0}^l u_{r+\sigma-\lambda} v_{\lambda} = c_{\sigma}, \quad 1 \leq \sigma \leq s.$$

Außerdem setzen wir im folgenden stets $c_s = c$; $c \neq 0$, weil $C(z)$ und $B(z) = z^s$ teilerfremd sind.

Beweis des Satzes 13. Zu (1): Wir führen für alle Paare aus $\mathfrak{P}_{m\tau k}(x)$ die Transformation $\zeta = z - b$ durch. Hierbei gehen $B(z)$ bzw. $C(z)$ in $B(\zeta) = B(\zeta + b) = B^*(\zeta)$ bzw. $C(\zeta) = C^*(\zeta)$ über. Setzt man weiter

$$f_i(z) = f_i(\zeta + b) = f_i^*(\zeta), \quad i = 1, 2;$$

$$g(z) = g(\zeta + b) = g^*(\zeta) = \zeta^r + \tau_1 \zeta^{r-1} + \cdots + \tau_r,$$

so geht (9) über in

$$(27.1) \quad f_1^*(\zeta)f_2^*(\zeta) = B^*(\zeta)g^*(\zeta) + C^*(\zeta).$$

⁵⁾ Alle vorkommenden Abschätzungen haben die Form $\psi(x) = x^{\alpha} \log^{\beta} x$ mit $\alpha, \beta \geq 0$.

Aus

$$z^r + t_1 z^{r-1} + \dots + t_r = (z - b)^r + \tau_1 (z - b)^{r-1} + \dots + \tau_r$$

ergibt sich

$$t_\varrho = \sum_{i=0}^r b_{\varrho i} \tau_i, \quad 0 \leq \varrho \leq r, \quad \text{mit den in (25.2) definierten } b_{\varrho i} \text{ und } \tau_0 = 1.$$

Die Bedingung (N) geht daher über in

$$(N^*) \quad \sum_{\varrho=0}^r \left(\sum_{i=0}^r b_{\varrho i} \tau_i \right)^2 \leq x^2.$$

Da die Transformation $\zeta = z - b$ umkehrbar eindeutig ist, ist die Anzahl der Paare $f_1^*(\zeta)$, $f_2^*(\zeta)$, die den Bedingungen (27.1) und (N*) genügen, gleich der Anzahl $P_{m\tau k}(x)$. Sie ist aber andererseits auch gleich der Anzahl $P_{m\tau k}^{**}(x)$, wie man durch entsprechende Änderung der Bezeichnungen erkennt.

Zu (2): Setzt man

$$B_{ij} = \sum_{\varrho=0}^r b_{\varrho i} b_{\varrho j},$$

so bilden die B_{ij} eine positiv-definite Matrix und es gilt für jedes Polynom $g(z)$

$$(27.2) \quad \gamma_9^2 N(g)^2 \leq \sum_{\varrho=0}^r \left(\sum_{i=0}^r b_{\varrho i} t_i \right)^2 = \sum_{i,j=0}^r B_{ij} t_i t_j \leq \gamma_{10}^2 N(g)^2.$$

Aus Satz 1 folgt dann

$$1 \leq N(f_1) N(f_2) \leq \gamma N(g) \leq \frac{\gamma}{\gamma_9} \left(\sum_{\varrho=0}^r \left(\sum_{i=0}^r b_{\varrho i} t_i \right)^2 \right) \leq \gamma'' x.$$

Zu (3): Wegen 27.2) ist $P_{m\tau k}^*(x) \leq P_{m\tau k}^{**}(\gamma_{10}x) = P_{m\tau k}(\gamma_{10}x)$. Aus $P_{m\tau k}(x) = O(\psi(x))$ folgt daher $P_{m\tau k}^*(x) = O(\psi(\gamma_{10}x)) = O(\psi(x))^6$.

Satz 14. Falls $B(z) = (z - b)^s$, ist für beliebiges m ⁷⁾

$$P_{m,\tau,\tau-1}(x) = O(x^{r-2}) \text{ für } r \geq 4; \quad P_{m42}(x) = O(x^2).$$

Beweis. Wir nehmen $B(z) = z^s$ an (s. Folgerung zu Satz 13). Daher muß u_k einer der endlich vielen Teiler von c sein.

Aus dem Satz 3 folgt

$$\begin{aligned} P_{m\tau k}(x) &= O\left(x^{r-k} \sum_{d|c} \sum_{1 \leq 1+d^2+u_1^2+\dots+u_{k-1}^2 \leq (\gamma x)^2} (1+d^2+u_1^2+\dots+u_{k-1}^2)^{-\frac{r-k}{2}}\right) \\ &= O\left(x^{r-k} \sum_{d|c} \int_1^{\gamma x} u^{k-2} (1+d^2+u^2)^{-\frac{r-k}{2}} du\right) = O\left(x^{r-k} \int_1^{\gamma x} u^{2k-r-2} du\right) \end{aligned}$$

und hieraus die Behauptung.

⁶⁾ Siehe Anm. 5.

⁷⁾ Wie der Beweis zeigt, genügt es vorauszusetzen, daß $B(z)$ einen ganzzahligen Linearfaktor hat, was sich auf den Fall $B(z) = z B_1(z)$ zurückführen läßt.

Jetzt können wir auch den noch verbliebenen Fall $m = 5$, $s = 1$ der Gleichung (5.7) des Hauptsatzes 1 erledigen.

Da nur $B(z) = z - b$ möglich ist, folgt aus (20) und Satz 14:

$$R_{51}(x) = P_{541}(x) + O(P_{542}(x)) + O(P_{54}(x)) = P_{541}(x) + O(x^2)$$

und hieraus (5.7) mit Hilfe des Satzes 9.

V.

Um die Anzahlen $P_{mrk}(x)$ im Falle $k = r$ und später im Falle $k = r + 1$ abschätzen zu können, erweisen sich die beiden folgenden Sätze als nützlich.

Satz 15. Für $n = 1$ und $n \geq 3$ sei $L_n(x)$ die Anzahl der $n + 1$ -tupel ganzer Zahlen $U_1, U_2, \dots, U_n, V$, die den Bedingungen

$$(28.1) \quad AU_1 + BV = C;$$

$$(28.2) \quad (1 + U_1^2 + \dots + U_n^2)(1 + V^2) \leq x^2$$

genügen, wobei A, B und C feste ganze Zahlen sind. Dann gilt

$$L_1(x) = O(x^{1/2}) \quad \text{und} \quad L_n(x) = O(x^{n-1}) \quad \text{für } n \geq 3.$$

Beweis. Wir können uns auf den Fall beschränken, daß (28.1) ganzzahlige Lösungen besitzt.

Im Falle $n = 1$ ist $L_1(x)$ gleich der Anzahl der ganzen Zahlen U , welche der Bedingung

$$(28.3) \quad (1 + U^2)(B^2 + (C - AU)^2) \leq B^2x^2$$

genügen, also ein $O(x^{1/2})$.

Für $n \geq 3$ folgen aus (28.2) die Ungleichungen

$$(28.4) \quad 1 + U_2^2 + \dots + U_n^2 \leq x^2 \quad \text{und} \quad v^2 \leq x^2(1 + U_2^2 + \dots + U_n^2)^{-1}.$$

U_1 ist wegen (28.1) durch V eindeutig bestimmt. Ist daher $L'_n(x)$ die Anzahl der n -tupel $U_2, \dots, U_n$, die die Ungleichungen (28.4) erfüllen, so ist gewiß $L_n(x) \leq L'_n(x)$ und

$$\begin{aligned} L'_n(x) &= \sum_{1 + U_2^2 + \dots + U_n^2 \leq x^2} \{2[x(1 + U_2^2 + \dots + U_n^2)^{-1/2}] + 1\} \\ &= 2xO\left(\int_1^x u^{n-2}(1 + u^2)^{-1/2} du\right) + O(x^{n-1}) = O(x^{n-1}). \end{aligned}$$

Satz 16. $A \neq 0$ sei eine beliebige ganze Zahl, $\varphi(v)$ eine für alle ganzen Zahlen eines bestimmten (endlichen oder unendlichen) Intervalls definierte eindeutige Funktion. $\mathfrak{L}_2(x)$ sei die Menge, $L_2(x)$ die Anzahl der Paare ganzer Zahlen u, v , für welche $\varphi(v)$ ganzzahlig ist und die Ungleichung

$$(29) \quad (u^2 + v^2)(v^2 + (Au - \varphi(v))^2) \leq x^2$$

gilt. Dann ist

$$L_2(x) = O(x).$$

Beweis. Der Einfachheit halber schreiben wir während des ganzen Beweises φ statt $\varphi(v)$.

Für die Paare u, v aus $\mathfrak{L}_2(x)$ mit $Au\varphi \leq 0$ gilt:

$$(u^2 + v^2)(v^2 + (Au - \varphi)^2) \geq (u^2 + v^2)(v^2 + A^2u^2) \geq (u^2 + v^2)^2.$$

Wegen (29) ist ihre Anzahl also ein $O(x)$.

Für ein festes ganzzahliges v sei $\mathfrak{L}(x, v)$ die Menge, $Q(x, v)$ die Anzahl der Paare u, v , welche die Bedingungen

$$(30) \quad Au\varphi > 0, \quad |v| \leq x^{1/2} \quad \text{und} \quad |u| |Au - \varphi| \leq x$$

erfüllen. Da (30.2) und (30.3) aus (29) folgen, gilt

$$(31) \quad L_2(x) = \sum_{|v| \leq \sqrt{x}} Q(x, v) + O(x).$$

Zur Abschätzung der Anzahlen $Q(x, v)$ müssen mehrere Fälle unterschieden werden. Hierbei ist jedesmal zu beachten, daß u bei festem v wegen (30.1) entweder nur positive oder nur negative Werte annehmen kann.

Ist $|Au| \geq |\varphi|$, so geht (30.3) über in $u^2 - A^{-1}u\varphi \leq |A|^{-1}x$, also $|u| - |(2A)^{-1}\varphi|^2 \leq (2A)^{-2}\varphi^2 + |A|^{-1}x$, oder wegen $|Au| \geq |\varphi|$ in

$$|A^{-1}\varphi| \leq |u| \leq |(2A)^{-1}\varphi| + ((2A)^{-2}\varphi^2 + |A|^{-1}x)^{1/2}.$$

Die Anzahl der Paare u, v aus $\mathfrak{L}(x, v)$ mit $|Au| \geq |\varphi|$ ist somit kleiner oder gleich

$$((2A)^{-2}\varphi^2 + |A|^{-1}x)^{1/2} - |(2A)^{-1}\varphi| + 1 \leq (|A|^{-1}x)^{1/2} + 1.$$

Ist $|Au| < |\varphi|$ und $|\varphi| < 2(|A|x)^{1/2}$, so folgt hieraus

$$(1 \leq) |u| < 2(|A|^{-1}x)^{1/2}.$$

Daher gilt

$$(32.1) \quad Q(x, v) \leq 3(|A|^{-1}x)^{1/2} + 1, \text{ falls } |\varphi| < 2(|A|x)^{1/2}.$$

Ist $|Au| < |\varphi|$ und $|\varphi| \geq 2(|A|x)^{1/2}$, so geht (30.3) über in

$$A^{-1}u\varphi - u^2 \leq |A|^{-1}x,$$

also $(|u| - |(2A)^{-1}\varphi|)^2 \geq (2A)^{-2}\varphi^2 - |A|^{-1}x (\geq 0)$. Hieraus ergibt sich, daß u entweder die Ungleichung

$$(1 \leq) |u| \leq |(2A)^{-1}\varphi| - ((2A)^{-2}\varphi^2 - |A|^{-1}x)^{1/2} \leq (|A|^{-1}x)^{1/2}$$

oder

$$|(2A)^{-1}\varphi| + ((2A)^{-2}\varphi^2 - |A|^{-1}x)^{1/2} \leq |u| < |A^{-1}\varphi|$$

erfüllen muß. Die Anzahl der u , welche der letzten Ungleichung genügen, ist kleiner oder gleich

$$|(2A)^{-1}\varphi| - ((2A)^{-2}\varphi^2 - |A|^{-1}x)^{1/2} + 1 \leq (|A|^{-1}x)^{1/2} + 1.$$

Hieraus folgt

$$(32.2) \quad Q(x, v) \leq 2(|A|^{-1}x)^{1/2} + 1, \text{ falls } |\varphi| \geq 2(|A|x)^{1/2}.$$

Wegen (32.1) und (32.2) ist $Q(x, v) \leq 3(|A|^{-1}x)^{1/2} + 1$ für beliebiges v , woraus wegen (31) sofort die Behauptung folgt.

Satz 17. Falls $B(z) = (z - b)^s$, ist für beliebiges m ⁸⁾

$$P_{m22}(x) = O(x^{1/2}); \quad P_{mrr}(x) = O(x^{r-2}) \text{ für } r \geq 3.$$

Beweis. Gemäß der Folgerung zu Satz 13 nehmen wir $B(z) = z^s$ an. Wegen $r = k \leq l = s$ ist $s \geq 2$. Die drei letzten Gleichungen von (26) lauten:

$$(33.1) \quad u_r v_l = c$$

$$(33.2) \quad u_r v_{l-1} + u_{l-1} v_l = c_{s-1}$$

$$(33.3) \quad u_r v_{l-2} + u_{r-1} v_{l-1} + u_{r-2} v_l = c_{s-2}.$$

Wegen (33.1) sind nur folgende Gleichungen zu beweisen:

$$Q_{m22}(x) = O(x^{1/2}); \quad Q_{mrr}(x) = O(x^{r-2}) \text{ für } r \geq 3,$$

wobei $Q_{mrr}(x)$ für $r \geq 2$ die Anzahl der Paare $f_1(z), f_2(z)$ aus $\mathfrak{P}_{mrr}(x)$ bedeuten soll, welche die Bedingungen (33) und (N') erfüllen und bei welchen u_r ein fester Teiler von c ist. Ist $r \neq 3$, so folgern wir aus (N')

$$(1 + u_1^2 + \dots + u_{r-1}^2)(1 + v_{l-1}^2) \leq (\gamma x)^2.$$

Dann sind für $n = r - 1$, $u_r = B$, $v_1 = A$, $u_{r-i} = U_i$, $1 \leq i \leq r - 1$, $v_{l-1} = V$, $c_{s-1} = C$ die Bedingungen des Satzes 15 erfüllt und

$$Q_{mrr}(x) \leq L_{r-1}(\gamma x).$$

Es sei nun $r = 3$. Wir wählen einen festen Teiler $u_3 = d$ von c und setzen $v_l = e$, $u_1 = u$, $u_2 = v$. Dann folgt aus (33):

$$dv_{l-1} = c_{s-1} - ev, \quad d^2 v_{l-2} = -cu + \varphi(v) \text{ mit } \varphi(v) = ev^2 - c_{s-1}v + dc_{s-2},$$

ferner

$$\begin{aligned} d^4(1 + v_{l-2}^2 + v_{l-1}^2) &= d^4 + d^2(c_{s-1} - ev)^2 + (cu - \varphi(v))^2 \\ &\geq \gamma_{11}v^2 + (cu - \varphi(v))^2 \geq \gamma_{12}(v^2 + (cu - \varphi(v))^2) \end{aligned}$$

sowie

$$d^4 N(f_1)^2 N(f_2)^2 \geq \gamma_{12}(u^2 + v^2)(v^2 + (cu - \varphi(v))^2).$$

aus (N') folgt dann

$$(u^2 + v^2)(v^2 + (cu - \varphi(v))^2) \leq (\gamma_{13}x)^2.$$

Da $c \neq 0$, $\varphi(v)$ die Bedingungen des Satzes 16 erfüllt und zu jedem Paar u, v höchstens ein Paar $f_1(z), f_2(z)$ aus $\mathfrak{P}_{m33}(x)$ gehört, gilt

$$Q_{m33}(x) \leq L_2(\gamma_{13}x) = O(x).$$

⁸⁾ Ähnlich wie bei Anm. 7 genügt es vorauszusetzen, daß $B(z)$ für $r \neq 3$ eine ganzzahlige Doppelwurzel bzw. für $r = 3$ eine ganzzahlige dreifache Wurzel hat.

VI.

Satz 18. Falls $B(z) = (z - b)^s$, ist für beliebiges m

$$P_{m12}(x) = O(1); \quad P_{m23}(x) = O(x^{1/2});$$

$$P_{m,r,r+1}(x) = O(x^{r-2}) \text{ für } r \geq 3.$$

Beweis. Wir nehmen wieder $B(z) = z^s$ an (siehe Folgerung zu Satz 13). Dann ist u_{r+1} wiederum ein Teiler von c . Nach Satz 6 ist $f_2(z)$ durch $f_1(z)$ eindeutig bestimmt und das Gleichungssystem (26) muß die Lösung $v_0 = 1$ haben, weshalb gilt:

$$\begin{vmatrix} c_1 & u_r & \cdots & 1 & 0 & \cdots & 0 \\ c_2 & u_{r+1} & \cdots & 1 & 0 & \cdots & 0 \\ c_3 & 0 & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & 1 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ c & 0 & \cdots & \cdots & 0 & \cdots & u_{r+1} \end{vmatrix} - u_{r+1}^s = 0.$$

Bei fest gewähltem $u_{r+1} = d|c$ ist die linke Seite dieser Gleichung ein Polynom $D(u_1, \dots, u_r)$ in r Veränderlichen.

Es kann nicht identisch verschwinden, da es $(-1)^s c u_r^{s-1} \neq 0$ als Glied enthält.

Ist $r = 1$, so folgt aus $D(u_1) = 0$, daß diese Gleichung bei festem $u_2 = d$ höchstens $s - 1$ ganzzahlige Lösungen u_1 hat, d. h.

$$(34) \quad P_{m12}(x) \leq (s - 1) 2 T(c) = O(1).$$

Es sei nun $r \geq 2$. ($s - 1 = l \geq k \geq 3$). Wir denken uns $D(u_1, \dots, u_r)$ in irreduzible Faktoren zerlegt:

$$D(u_1, \dots, u_r) = \prod_{\nu=1}^n F_{\nu}(u_{q_{\nu}}, \dots, u_r), \quad n \leq s - 1, \quad q_{\nu} \geq 1,$$

wobei $u_{q_{\nu}}$ in jedem Polynom F_{ν} tatsächlich vorkommen soll. Jedes Polynom $f_1(z)$ aus $\mathfrak{M}_{r+1}$ muß also für mindestens ein ν die Bedingung

$$F_{\nu}(u_{q_{\nu}}, \dots, u_r) = 0$$

erfüllen.

Für den weiteren Verlauf dieses Beweises sei $\mathfrak{D}_{mr}(x)$ die Menge, $Q_{mr}(x)$ die Anzahl der Paare ganzzahliger Polynome $f_1(z), f_2(z)$ mit folgenden Eigenschaften: u_{r+1} ist ein fester Teiler d von c ; die Koeffizienten von $f_1(z)$ und $f_2(z)$ erfüllen die Bedingungen (N') und (26) sowie

$$(35) \quad F(u_q, \dots, u_r) = 0, \quad 1 \leq q \leq r, \quad r \geq 2,$$

wobei F ein irreduzibles Polynom ist, das von u_q tatsächlich abhängt. Da sowohl c als auch $D(u_1, \dots, u_r)$ nur endlich viele Teiler haben, genügt es zum Beweis der Behauptung zu zeigen:

$$(36) \quad Q_{m_2}(x) = O(x^{1/2}); \quad Q_{m_r}(x) = O(x^{r-2}) \text{ für } r \geq 3.$$

Hierzu werden von den Gleichungen (26) folgende benötigt:

$$(37.1) \quad dv_{l-1} + u_r e = c_{s-1}$$

$$(37.2) \quad dv_{l-2} + u_r v_{l-1} + u_{r-1} e = c_{s-2} \quad \left(e = \frac{c}{d} \right)$$

$$(37.3) \quad dv_{l-3} + u_r v_{l-2} + u_{r-1} v_{l-1} + u_{r-2} e = c_{s-3}.$$

Weiter sei

$$(38) \quad F(u_q, \dots, u_r) = G_0 u_q^p + G_1 u_q^{p-1} + \dots + G_p, \quad 1 \leq p \leq s-1;$$

Hierbei sind die G_i Polynome in den Veränderlichen $u_{q'}, \dots, u_r$ mit $q' > q$ bzw. Konstanten, falls $q = r$. Die G_i dürfen nicht sämtlich verschwinden, insbesondere G_p nicht, da F irreduzibel ist.

a) Ist $q = r$, so hat (35) höchstens dann eine ganzzahlige Lösung u_r , wenn $p = 1$. Wegen (37.1) ist dann v_{l-1} durch u_r eindeutig bestimmt, während $u_1, \dots, u_{r-1}$ beliebige Werte annehmen können, welche den Bedingungen (N') und (26) speziell also (37.2) und

$$(39.1) \quad (1 + u_1^2 + \dots + u_{r-1}^2) (1 + v_{l-2}^2) \leq \gamma^2 x^2$$

genügen. Die letzten beiden Bedingungen gehen für $r \neq 3$ in die Bedingungen des Satzes 15 über, wenn man $r-1 = n$, $d = B$, $e = A$, $c_{s-2} - u_r v_{l-1} = C$, $v_{l-2} = V$ und $u_\varrho = U_{r-\varrho}$, $1 \leq \varrho \leq r-1$, setzt. Da zu jedem $r-1$ -tupel $u_1, \dots, u_{r-1}$ höchstens ein Paar $f_1(z)$, $f_2(z)$ aus $\mathfrak{Q}_{mr}(x)$ gehört, ergibt sich $Q_{mr}(x) \leq L_{r-1}(\gamma x)$ und (36) ist im Falle $q = r \neq 3$ bewiesen.

Für $q = r = 3$ folgt aus (37.2) und (37.3) bei festem u_3 und v_{l-1} :

$$dv_{l-2} = -eu_2 + D_1 \quad \text{mit} \quad D_1 = c_{s-2} - u_3 v_{l-1}$$

$$d^2 v_{l-3} = -cu_1 + D_2 u_2 + D_3 \quad \text{mit} \quad D_2 = eu_3 - dv_{l-1}; \quad D_3 = -D_1 u_3 + dc_{s-3}$$

und weiter

$$\begin{aligned} d^4 N(f_2)^2 &\geq d^4 (1 + v_{l-3}^2 + v_{l-2}^2) = (cu_1 - D_2 u_2 + D_3)^2 + d^4 + d^2 (eu_2 - D_1)^2 \\ &\geq \gamma_{14}^2 (u_1^2 + u_2^2), \end{aligned}$$

also wegen (N')

$$u_1^2 + u_2^2 \leq N(f_1) d^2 \gamma_{14}^{-1} N(f_2) \leq \gamma_{15} x.$$

Da zu jedem Paar u_1, u_2 höchstens ein Paar $f_1(z)$, $f_2(z)$ aus $\mathfrak{Q}_{mr}(x)$ gehört, gilt (36) auch für $q = r = 3$.

b) Wir nehmen nun an, die Gültigkeit von (36) sei im Falle $r \neq 3$ für jedes Polynom $F(u_{q'}, \dots, u_r)$ mit $q' > q$ bereits bewiesen und führen den Beweis für $F(u_q, \dots, u_r)$.

Zunächst sei $Q'_{m\tau}(x)$ die Anzahl der Paare $f_1(z), f_2(z)$ aus $\mathfrak{D}_{m\tau}(x)$, welche zu denjenigen $r-1$ -tupeln $u_1, \dots, u_{q-1}, u_{q+1}, \dots, u_r$ gehören, für die in (38) sämtliche $G_i, 0 \leq i \leq p$, verschwinden. Diese u_ϱ genügen dann auch der nicht identisch verschwindenden Gleichung $G_p = 0$ und somit auch einer irreduziblen Gleichung $G_{p\nu}(u_{q'_\nu}, \dots, u_r) = 0$ mit $q'_\nu > q$. Da (36) für $q' > q$ als bewiesen angenommen ist und im Falle $r = 2$ wegen der Irreduzibilität von F für ein u_2 nicht alle G_i gleichzeitig verschwinden können, ist

$$Q'_{m2}(x) = 0, \quad Q'_{m\tau}(x) = O(x^{r-2}) \quad \text{für } r \geq 4.$$

Ist für ein $r-1$ -tupel $u_1, \dots, u_{q-1}, u_{q+1}, \dots, u_r$ mindestens ein $G_i \neq 0$, so gibt es hierzu höchstens p ganzzahlige Werte u_q , welche die Gleichung (35) erfüllen, also auch höchstens p Paare $f_1(z), f_2(z)$ aus $\mathfrak{D}_{m\tau}(x)$. Ferner gelten dann die Gleichungen (37.1) und wegen (N') auch die Ungleichung

$$(39.2) \quad (1 + u_1^2 + \dots + u_{q-1}^2 + u_{q+1}^2 + \dots + u_r^2) (1 + v_{l-1}^2) \leq \gamma^2 x^2.$$

Die letzten beiden Bedingungen gehen in die des Satzes 15 über, wenn man $r-1 = n, d = B, e = A, c_{s-1} = C, v_{l-1} = V$ und $u_\varrho = U_{r+1-\varrho}$ für $q+1 \leq \varrho \leq r, u_\varrho = U_{r-\varrho}$ für $1 \leq \varrho \leq q-1$ setzt. Hieraus folgt für beliebiges q

$$Q_{m2}(x) \leq p L_1(\gamma x) = O(x^{1/2})$$

$$Q_{m\tau}(x) \leq p L_{r-1}(\gamma x) + Q'_{m\tau}(x) = O(x^{r-2}) \quad \text{für } r \geq 4.$$

c) Es bleiben noch die Fälle $r = 3, q = 2$ und $r = 3, q = 1$. Im erstgenannten sei $u_1 = u, u_2 = w, u_3 = v$ gesetzt.

(35) und (38) gehen über in

$$(40) \quad F(w, v) = G_0(v) w^p + G_1(v) w^{p-1} + \dots + G_p(v) = 0, \quad 1 \leq p \leq s-1,$$

wobei die $G_i(v)$ für keinen Wert v sämtlich verschwinden können, da $F(w, v)$ sonst reduzibel wäre. Betrachten wir v für den Augenblick als reelle Veränderliche, so gibt es endlich viele (höchstens p) eindeutige, jeweils für ein bestimmtes Intervall definierte Funktionen $q_j(v)$, so daß die ganzzahligen Lösungen von (40) die Paare $v, q_j(v)$ mit ganzzahligem v und $q_j(v)$ sind. Aus den Gleichungen (37) folgt nun

$$d v_{l-1} = c_{s-1} - e v; \quad d^3 v_{l-3} = H_1(v) + H_2(v) w - c d u$$

mit $H_1(v) = -e v^3 + c_{s-1} v^2 - d c_{s-2} v + d^2 c_{s-3}$ und $H_2(v) = 2 c v - d c_{s-1}$ und hieraus für festes j , wenn man $\bar{q}_j(v) = H_1(v) + H_2(v) q_j(v)$ setzt:

$$\begin{aligned} d^6 N(f_2)^2 &\geq d^6 (1 + v_{l-1}^2 + v_{l-3}^2) = d^6 + d^4 (e v - c_{s-1})^2 + (c d u - \bar{q}_j(v))^2 \\ &\geq \gamma_{16} (v^2 + (c d u - \bar{q}_j(v))^2) \end{aligned}$$

und mit Hilfe von (N')

$$(u^2 + v^2) (v^2 + (c d u - \bar{q}_j(v))^2) \leq d^6 \gamma_{16}^{-1} N(f_1)^2 N(f_2)^2 \leq \gamma_{17}^2 x^2.$$

Da $\bar{q}_j(v)$ die Bedingung für die Funktion $q(v)$ des Satzes 16 erfüllt und zu jedem Paar u, v höchstens p Paare $f_1(z), f_2(z)$ aus $\mathfrak{D}_{m3}(x)$ gehören, ergibt

sich

$$Q_{m3}(x) \leq p L_2(\gamma_{17} x) = O(x), \quad \text{falls } q = 2.$$

d) Im Falle $q = 1$, $r = 3$ sei $u_1 = w$, $u_2 = u$, $u_3 = v$ gesetzt.

Verschwinden in (38) die G_i für ein Paar u, v sämtlich, so kann man dies völlig analog zum ersten Teil von b) auf einen der bereits bewiesenen Fälle $q = 2$ oder $q = 3$ zurückführen. Zu den Paaren u, v , für welche mindestens ein G_i nicht verschwindet, gibt es höchstens p ganzzahlige Werte w , also jeweils höchstens p Paare $f_1(z), f_2(z)$ aus $\mathfrak{D}_{m3}(x)$. Aus den Gleichungen (37) folgt wie im Beweis des Satzes 17 für $r = 3$

$$(u^2 + v^2)(v^2 + (cu - \varphi(v))^2) \leq (\gamma_{18} x)^2$$

und nach Satz 16

$$Q_{m3}(x) \leq p L_2(\gamma_{18} x) = O(x) \quad \text{auch für } q = 1.$$

Die Gleichungen (8.1), (8.3) und (8.7) des Hauptsatzes 3 ergeben sich nun folgendermaßen:

Aus $s \leq \frac{m+3}{2}$ folgt $m \leq 2r + 3$ und $\left[\frac{m}{2}\right] \leq r + 1$. Die genannten Gleichungen erhält man daher sofort aus (20) mit Hilfe der Sätze 9, 10, 7, 14, 17 und 18.

VII.

Der Fall $B(z) = (z - b)^s$, $r = 3$, $k = 2$ muß gesondert behandelt werden.

Satz 19. r_1 und r_2 seien zwei rationale Zahlen mit $r_2 > 0$ und $\varphi(y)$ eine für $-\infty < y < +\infty$ definierte stetige Funktion mit folgenden Eigenschaften: $\varphi(y)$ ist streng monoton für $|y| \geq y_0 > 0$, und es gibt eine natürliche Zahl s , so daß

$$(41.1) \quad \gamma_{19} y^{2s} \leq \varphi(y) \leq \gamma_{20} y^{2s} \quad \text{für alle } y \text{ mit } |y| \geq y_0 > 0.$$

Dann ist

$$\sum_{\varphi(y) \leq x^2} ((y - r_1)^2 + r_2)^{-1/2} (x^2 - \varphi(y))^{1/2} = 2s^{-1} x \log x + O(x).$$

Hierbei wird über alle ganzen Zahlen y summiert, für welche die Bedingung $\varphi(y) \leq x^2$ gilt.

Beweis. Aus den Eigenschaften der Funktion $\varphi(y)$ folgt, falls $x > x_0 = \max(\varphi(y); |y| \leq y_0)$, die Existenz von genau zwei Zahlen $\xi_1 > 0$ und $\xi_2 > 0$ derart, daß

$$\varphi(\xi_1) = \varphi(-\xi_2) = x^2.$$

Dann ist wegen (41.1)

$$\gamma_{19} \xi_i^{2s} \leq x^2 \leq \gamma_{20} \xi_i^{2s}, \quad i = 1, 2.$$

also

$$(41.2) \quad \gamma_{21} x^s \leq \xi_i \leq \gamma_{22} x^s, \quad i = 1, 2,$$

und weiter

$$\sum_{\varphi(y) \leq x^2} ((y-r_1)^2 + r_2)^{-1/2} (x^2 - \varphi(y))^{1/2} = \sum_{y=1}^{\xi_1} ((y-r_1)^2 + r_2)^{-1/2} (x^2 - \varphi(y))^{1/2} \\ + \sum_{y=-1}^{\xi_2} ((y+r_1)^2 + r_2)^{-1/2} (x^2 - \varphi(-y))^{1/2} + (r_1^2 + r_2)^{-1/2} (x^2 - \varphi(0))^{1/2}.$$

Da das letzte Glied ein $O(x)$ ist und die zweite Summe auf der rechten Seite aus der ersten hervorgeht, indem man r_1 durch $-r_1$ und y durch $-y$ ersetzt, genügt es zu zeigen

$$(42) \quad \sum_{y=1}^{\xi} ((y-r_1)^2 + r_2)^{-1/2} (x^2 - \varphi(y))^{1/2} = s^{-1} x \log x + O(x) \\ \text{für } \xi = \xi_1 \text{ und } \xi = \xi_2.$$

Zunächst ist

$$\sum_{y=1}^{\xi} |((y-r_1)^2 + r_2)^{-1/2} - y^{-1}| \\ = \sum_{y=1}^{\xi} y^{-1} ((y-r_1)^2 + r_2)^{-1/2} |y - ((y-r_1)^2 + r_2)^{1/2}| \\ \leq \gamma_{23} \sum_{y=1}^{\xi} y^{-2} \frac{|y^2 - (y-r_1)^2 - r_2|}{y + ((y-r_1)^2 + r_2)^{1/2}} \leq \gamma_{23} \sum_{y=1}^{\xi} y^{-3} |2r_1 y - r_1^2 - r_2| \\ \leq \gamma_{24} \sum_{y=1}^{\xi} y^{-2} = O(1).$$

Bezeichnet man die linke Seite von (42) mit S , so gilt

$$\left| S - \sum_{y=1}^{\xi} y^{-1} (x^2 - \varphi(y))^{1/2} \right| \leq x \sum_{y=1}^{\xi} |((y-r_1)^2 + r_2)^{-1/2} - y^{-1}| = x \cdot O(1) = O(x), \\ S = \sum_{y=1}^{\xi} y^{-1} (x^2 - \varphi(y))^{1/2} + O(x).$$

Weiter ist

$$x^2 \geq x^2 - \varphi(y) \geq (x^2 - \varphi(y)) (1 - \varphi(y) x^{-2}) = (x - \varphi(y) x^{-1})^2$$

und daher

$$0 \leq x \sum_{y=1}^{\xi} y^{-1} - \sum_{y=1}^{\xi} y^{-1} (x^2 - \varphi(y))^{1/2} \leq x^{-1} \sum_{y=1}^{\xi} y^{-1} \varphi(y) \leq \gamma_{20} x^{-1} \sum_{y=1}^{\xi} y^{2s-1} \\ = O\left(x^{-1} \int_1^{\xi} y^{2s-1} dy\right) = O(x^{-1} \xi^{2s}) = O(x),$$

letzteres wegen (41.2).

Hieraus folgt

$$\sum_{y=1}^{\xi} y^{-1} (x^2 - \varphi(y))^{1/2} = x \sum_{y=1}^{\xi} y^{-1} + O(x) = x (\log \xi + O(1)) + O(x) \\ = x \log \xi + O(x).$$

Ferner ergibt sich aus (41.2): $\log \xi = s^{-1} \log x + O(1)$, also

$$S = x (s^{-1} \log x + O(1)) + O(x) = s^{-1} x \log x + O(x).$$

Satz 20. Falls $B(z) = (z - b)^s$, ist

$$P_{432}(x) = 2\beta'_1(b, C) x \log x + O(x) \\ P_{m32}(x) = \beta'_s(b, C) x \log x + O(x) \quad \text{für } s \geq 2 \quad (m \geq 5)$$

mit den in (6) definierten Konstanten $\beta'_s(b, C)$.

Beweis. Nach Satz 13 bestimmen wir die Anzahl $P_{m32}^{**}(x)$, d. h. die Anzahl der Paare $f_1(z), f_2(z)$ der Grade $k = 2$ bzw. $l = m - 2$, welche die Bedingungen

$$(43) \quad f_1(z) f_2(z) = z^s g(z) + C^*(z)$$

mit

$$g(z) = z^3 + t_1 z^2 + t_2 z + t_3; \\ C^*(z) = C(z + b) = c_1^* z^{s-1} + \dots + c_{s-1}^* z + c; \\ f_1(z) = z^2 + u z + d, \quad d \mid c$$

sowie

$$(N_1) \quad 1 + (t_1 - 3b)^2 + (t_2 - 2bt_1 + 3b^2)^2 + (t_3 - bt_2 + b^2t_1 - b^3)^2 \leq x^2$$

erfüllen. Aus (14.3) und (14.1) folgt, wenn man noch $h(z) = z + t$ setzt:

$$g(z) = (z + t) f_1(z) + g'(z) \quad \text{mit} \quad g'(z) = t'_1 z + t'_2,$$

also

$$(44) \quad t_1 = t + u, \quad t_2 = ut + d + t'_1, \quad t_3 = dt + t'_2.$$

Wegen (44) geht (N_1) über in

$$(45) \quad G_0 t^2 + 2G_1 t + G_2 \leq x^2,$$

wobei G_0, G_1 und G_2 nur von b, u, d abhängen, weil auf Grund der Gleichungen (12.2) t'_1 und t'_2 durch u und d eindeutig bestimmt sind. Überdies sind G_0, G_2 und $G_0 G_2 - G_1^2$, also auch $G = G_0^{-1} (G_0 G_2 - G_1^2)$ positiv.

$P_{m32}^{**}(x)$ ist dann gleich der Anzahl der Paare $f_1(z), t$, für welche $f_1(z)$ zu $\mathfrak{M}_k$ gehört und t die Ungleichung (45) erfüllt, also bekanntlich

$$P_{m32}^{**}(x) = \sum_{\substack{f_1 \in \mathfrak{M}_k \\ G \leq x^2}} (2G_0^{-1/2} (x^2 - G)^{-1/2} + O(1)).$$

Wegen Satz 13, Behauptung (2) gilt

$$\sum_{f_1 \in \mathfrak{M}_k} 1 \leq \sum_{N(f_1) \leq \gamma'' x} 1 = \sum_{d \mid c} \sum_{1+u^2+d^2 \leq (\gamma'' x)^2} 1 = O(x)$$

und daher

$$(46) \quad P_{m32}(x) = P_{m32}^{**}(x) = 2 \sum_{\substack{f_1 \in \mathfrak{M}_k \\ G \leq x^2}} G_0^{-1/2}(x^2 - G)^{1/2} + O(x).$$

Es sei nun $s \geq 2$. Zur Bestimmung der Menge $\mathfrak{M}_k$ sei bemerkt, daß $f_1(z)$ genau dann zu $\mathfrak{M}_k$ gehört, wenn das zugehörige Gleichungssystem (12.2) ganzzahlige Lösungen v'_1 und v'_2 hat⁹⁾; denn dann sind, wie man leicht nachprüft, auch t'_1, t'_2 sowie $v'_3, \dots, v'_s$ ganzzahlig. Die Determinante des Systems (12.2) hat den Wert d^s . Man erhält daher, wie man ebenfalls leicht nachrechnet:

$$(47) \quad v'_1 = d^{-(s-1)} D_1(u), \quad v'_2 = d^{-(s-2)} D_2(u),$$

wobei $D_1(u)$ und $D_2(u)$ die in der Einleitung im Anschluß an den Hauptsatz 2 definierten Determinanten bedeuten. Diese sind Polynome in u und es folgt aus $u \equiv u' \pmod{d^{s-1}}$ auch $D_i(u) \equiv D_i(u') \pmod{d^{s-1}}$, $i = 1, 2$. Bei festem d sind daher v'_1 und v'_2 genau dann ganzzahlig für ein u , wenn dies für das zugehörige u' mit $u \equiv u' \pmod{d^{s-1}}$ und $0 \leq u' < |d|^{s-1}$ der Fall ist. Mit u_{dj} , $d \mid c$, $1 \leq j \leq q(d)$ seien die (endlich vielen) Werte bezeichnet, für welche gilt:

$$D_1(u_{dj}) \equiv 0 \pmod{d^{s-1}}, \quad D_2(u_{dj}) \equiv 0 \pmod{d^{s-2}}, \quad 0 \leq u_{dj} < |d|^{s-1}.$$

Dann ist $\mathfrak{M}_k$ die Menge der Polynome $f_1(z) = z^2 + uz + d$ mit

$$(48) \quad u = u_{dj} + d^{s-1}y, \quad d \mid c, \quad 1 \leq j \leq q(d), \quad y \text{ beliebig ganz.}$$

Aus (46) folgt dann

$$P_{m32}(x) = 2 \sum_{d \mid c} \sum_{j=1}^{q(d)} \left(\sum_{G \leq x^2} G_0(u_{dj}, y)^{-1/2} (x^2 - G(u_{dj}, y))^{-1/2} \right) + O(x),$$

wobei $G_0(u_{dj}, y)$ bzw. $G(u_{dj}, y)$ diejenigen Ausdrücke bedeuten sollen, welche man erhält, wenn man in $G_0(u)$ bzw. $G(u)$ den Wert u durch die sich aus (48) und t_1 und t_2 durch die sich aus (12.2) ergebenden Werte ersetzt. Wegen (7) ist nur der Nachweis folgender Tatsache notwendig:

Für jeden Teiler $d \mid c$ und jedes u_{dj} , $1 \leq j \leq q(d)$ gilt:

$$(49) \quad \sum_{G \leq x^2} G_0(u_{dj}, y)^{-1/2} (x^2 - G(u_{dj}, y))^{1/2} = 2s^{-1} (1 + b^2)^{-1/2} |d|^{1-s} x \log x + O(x),$$

wobei bei festem d und u_{dj} über alle möglichen ganzzahligen Werte von y summiert werden soll.

Zunächst ist

$$\begin{aligned} D_1(u) &= e u^{s-1} + O(|u|^{s-2}) = e d^{(s-1)2} y^{s-1} + O(|y|^{s-2}) \\ D_2(u) &= e u^{s-2} + O(|u|^{s-3}) = e d^{(s-1)(s-2)} y^{s-2} + O(|y|^{s-3}), \end{aligned}$$

wobei die Abschätzungen für $|u| \rightarrow \infty$ bzw. $|y| \rightarrow \infty$ gelten sollen, und aus

⁹⁾ Hierbei ist natürlich $B(z)$ durch z^s und $C(z)$ durch $C^*(z)$ zu ersetzen.

(47), (48), (12.2), (44) und (N_1) folgt

$$\begin{aligned} v'_1 &= t'_1 = e d^{(s-1)s-2} y^{s-1} + O(|y|^{s-2}) \\ v'_2 &= e d^{(s-2)^2} y^{s-2} + O(|y|^{s-3}) \\ t'_2 &= u v'_1 + v'_2 = e d^{(s-1)^2} y^s + O(|y|^{s-1}) \\ t_1 - 3b &= t + d^{s-1} y + u_{dj} - 3b = t + d^{s-1} y + O(1) \\ t_2 - 2b t_1 + 3b^2 &= (d^{s-1} y + u_{dj} - 2b) t + O(|y|^{s-1}) \\ t_3 - b t_2 + b^2 t_1 - b^3 &= (-b d^{s-1} y + d - b u_{dj} + b^2) t + e d^{(s-1)^2} y^s + O(|y|^{s-1}) \\ G_0(u_{dj}, y) &= 1 + (d^{s-1} y + u_{dj} - 2b)^2 + (b d^{s-1} y - d + b u_{dj} - b^2)^2 \\ &= (1 + b^2) d^{2(s-1)} ((y - r_1)^2 + r_2) = (1 + b^2) d^{2(s-1)} y^2 + O(|y|), \end{aligned}$$

wobei r_1 und r_2 gewisse rationale, nur von d , u_{dj} und b abhängige Zahlen mit $r_2 > 0$ sind.

$$\begin{aligned} G_1(u_{dj}, y) &= -b e d^{s(s-1)} y^{s+1} + O(|y|^s) \\ G_2(u_{dj}, y) &= e^2 d^{2(s-1)^2} y^{2s} + O(|y|^{2s-1}) \\ G_0 G_2 - G_1^2 &= e^2 d^{2s(s-1)} y^{2s+2} + O(|y|^{2s+1}). \end{aligned}$$

Aus der letzten Gleichung und dem Ausdruck für $G_0(u_{dj}, y)$ ergibt sich

$$G(u_{dj}, y) = e^2 (1 + b^2)^{-1} d^{2(s-1)^2} y^{2s} + O(|y|^{2s-1}).$$

$G(u_{dj}, y)$ erfüllt daher für jeden Teiler d von c und für jedes u_{dj} die Bedingungen für die Funktion $\varphi(y)$ des Satzes 19. Aus diesem Satz erhält man sofort die Gleichung (49).

Es sei nun $s = 1$, also $m = 4$. Dann ist $C^*(z) = c$, $f'_2(z) = v'_1 = \frac{c}{d} = e$, während $f_1(z) = z^2 + u z + d$ für beliebiges u zu $\mathfrak{M}_k$ gehört, falls $d \mid c$. Aus (12.2), (44) und (N_1) folgt, wobei die Abschätzungen für $|u| \rightarrow \infty$ gelten:

$$\begin{aligned} t'_1 &= v'_1 = e; \quad t'_2 = u v'_1 = e u \\ t_1 - 3b &= t + u - 3b \\ t_2 - 2b t_1 + 3b^2 &= (u - 2b) t - 2b u + O(1) \\ t_3 - b t_2 + b^2 t_1 - b^3 &= (-b u + d + b^2) t + (b^2 + e) u + O(1) \end{aligned}$$

und hieraus bei festem $d \mid c$, wenn wir nur die Abhängigkeit vor u eigens anführen:

$$\begin{aligned} G_0(u) &= 1 + (u - 2b)^2 + (b u - d - b^2)^2 \\ &= (1 + b^2) ((u - r_1)^2 + r_2) = (1 + b^2) u^2 + O(|u|) \quad \text{mit } r_2 > 0 \\ G_1(u) &= -b (b^2 + e + 2) u^2 + O(|u|) \\ G_2(u) &= (1 + 4b^2 + (b^2 + e)^2) u^2 + O(|u|) \\ G_0 G_2 - G_1^2 &= (1 + b^2 + (b^2 - e)^2) u^4 + O(|u|^3) \\ G(u) &= (1 + (b^2 - e)^2 (1 + b^2)^{-1}) u^2 + O(|u|). \end{aligned}$$

$G(u)$ erfüllt die Bedingungen der Funktion $\varphi(y)$ des Satzes 19 für $u = y$ und $s = 1$. Aus (46) folgt daher

$$\begin{aligned} P_{432}(x) &= 2 \sum_{d|c} \sum_{G \leq x^2} G_0(u)^{-1/2} (x^2 - G(u))^{1/2} + O(x) \\ &= 2 \sum_{d|c} (1+b^2)^{-1/2} \sum_{G \leq x^2} ((u-r_1)^2 + r_2)^{-1/2} (x^2 - G(u))^{1/2} + O(x) \\ &= 4 T(c) (1+b^2)^{-1/2} (2x \log x + O(x)) + O(x) \\ &= 2 \beta'_1(b, C) x \log x + O(x). \end{aligned}$$

Zum Beweis der Gleichung (8.5) des Hauptsatzes 3 seien noch folgende Vorbereitungen getroffen: $P'_{531}(x)$ bzw. $P'_{632}(x)$ seien die Anzahlen der Paare $f_1(z)$, $f_2(z)$, aus $\mathfrak{P}_{531}(x)$ bzw. $\mathfrak{P}_{632}(x)$, für welche $f_2(z)$ in zwei Faktoren vom Grade 2 zerlegt werden kann. Dann gilt der

Satz 21. Falls $B(z) = (z - b)^s$, ist

$$P'_{531}(x) = O(x^{1/2}); \quad P'_{632}(x) = O(x).$$

Beweis. Bei festem $f_1(z)$ gilt wegen (14.1, 2), und da man $B(z) = z^s$ wieder annehmen kann,

$$f_2(z) = z^s h(z) + f'_2(z),$$

wobei $f'_2(z)$ durch $f_1(z)$ eindeutig bestimmt ist, höchstens den Grad $s - 1$ besitzt und das konstante Glied $e = \frac{c}{d}$ mit $d = u_k$ hat. Bei festem $f_1(z)$ wird jedes reduzible $f_2(z)$ in derjenigen Anzahl $P_{422}(x)$ bzw. $P_{412}(x)$ mindestens einmal mitgezählt, die sich für die Polynome z^s (als $B(z)$) und $f'_2(z)$ (als $C(z)$) ergibt.

Im Falle $m = 5$, also $s = 2$, ist $f_1(z) = z + d$, $d | c$, und $h(z)$ vom Grade 2. Es gibt also nur endlich viele Polynome $f_1(z)$ aus $\mathfrak{M}_k$. Die Anzahl der zu jedem $f_1(z)$ gehörigen, in zwei quadratische Faktoren zerlegbaren Polynome $f_2(z)$ ist nach Satz 17 ein $O(x^{1/2})$, woraus wiederum folgt:

$$P'_{531}(x) = O(x^{1/2}).$$

Im Falle $m = 6$, also $s = 3$, ist $f_1(z) = z^2 + uz + d$, $d | c$, und $h(z)$ vom Grade 1. Wegen (34) gehören zu jedem Polynom $f_1(z)$ aus $\mathfrak{M}_k$ höchstens $2(s - 1) T(e)$ in zwei quadratische Faktoren zerlegbare Polynome $f_2(z)$. Aus (N') ergibt sich

$$u^2 \leq N(f_1)^2 \leq \gamma^2 x^2,$$

also

$$P'_{632}(x) \leq \sum_{|u| \leq \gamma x} \sum_{d|c} (s - 1) T(e) = O(x).$$

Weiter benötigen wir den

Satz 22. $P'_{mr}(x)$ sei für $r \geq 3$ die Anzahl der Paare $f_1(z), f_2(z)$ aus $\mathfrak{P}_{mr2}(x)$ mit $f_1(z) = (z - u)^2$. Dann ist

$$P'_{mr}(x) = O(x^{r-2}) \quad \text{für } r \geq 3.$$

Beweis. Wendet man den Satz 3 unter der Zusatzbedingung

$$f_1(z) = (z - u)^2$$

und unter Verzicht auf die Bedingung $f_1(z) \in \mathfrak{M}_k$ an, so erhält man sofort die Behauptung wegen $k = 2$ und

$$\sum_{1 \leq (N(z-u)^2) \leq \gamma x} (N(z-u)^2)^{-(r-2)} \leq \sum_{1+u^2 \leq \gamma x} (1+u^2)^{-1} = O(1).$$

Die Gleichungen (8.5) des Hauptsatzes 3 kann man jetzt folgendermaßen erhalten:

Es sei zunächst $m = 4$. Jedes reduzible Polynom $f(z)$ aus $\mathfrak{R}_{41}(x)$, das in zwei verschiedene irreduzible Faktoren zerlegt werden kann, wird entweder genau einmal in der Paarmenge $\mathfrak{P}_{431}(x)$ oder genau zweimal in der Paarmenge $\mathfrak{P}_{432}(x)$ mitgezählt. Kann $f(z)$ in zwei gleiche irreduzible Faktoren zerlegt werden, so wird es in $\mathfrak{P}_{432}(x)$ genau einmal mitgezählt, und zwar bei denjenigen Paaren, für welche $f_1(z) = f_2(z)$. Für diese gilt aber nach Satz 1: $N(f_1)^2 = 1 + u_1^2 + u_2^2 \leq \gamma x$, weshalb ihre Anzahl ein $O(x)$ ist.

Läßt sich ein Polynom aus $\mathfrak{R}_{41}(x)$ in drei oder vier irreduzible Faktoren zerlegen, so wird es mindestens einmal in einer der Anzahlen $P_{43}(x)$ oder $P'_{43}(x)$ mitgezählt; diese sind aber nach den Sätzen 10 und 22 jeweils ein $O(x)$. Aus diesen Überlegungen folgt

$$R_{41}(x) = P_{431}(x) + \frac{1}{2} P_{432}(x) + O(x)$$

und hieraus mit Hilfe der Sätze 9 und 20 die Gleichung (8.5) für $m = 4$.

Wegen $s \leq \frac{m+3}{2}$ und $s = m - 3$ ist $m \leq 9$. In den somit verbleibenden Fällen $5 \leq m \leq 9$ wird jedes reduzible Polynom aus $\mathfrak{R}_{m,m-3}(x)$, das sich in zwei irreduzible Faktoren zerlegen läßt, entweder genau einmal in $\mathfrak{P}_{m31}(x)$ oder genau einmal in $\mathfrak{P}_{m32}(x)$ oder ein- oder zweimal in einer der Mengen $\mathfrak{P}_{m3k}(x)$, $3 \leq k \leq \left[\frac{m}{2} \right]$, mitgezählt. Läßt sich ein Polynom aus $\mathfrak{R}_{m,m-3}(x)$ in mehr als zwei irreduzible Faktoren zerlegen, so wird es mindestens je einmal in einer der Anzahlen $P_{m3}(x)$, $P'_{m3}(x)$, $5 \leq m \leq 9$, oder $P_{m3k}(x)$, $3 \leq k \leq \left[\frac{m}{2} \right]$, oder $P'_{531}(x)$ oder $P'_{632}(x)$ mitgezählt. Hieraus folgt mit Hilfe der Sätze 17, 18, 10, 22 und 21

$$R_{m,m-3}(x) = P_{m31}(x) + P_{m32}(x) + O(x) \quad \text{für } 5 \leq m \leq 9$$

und (8.5) aus den Sätzen 9 und 20, womit auch der Hauptsatz 3 vollständig bewiesen ist.

Lebenslauf

Als Sohn des Bankbeamten Friedrich Grummich und seiner Ehefrau Anna, geb. Czech, wurde ich, Friedrich Grummich, am 23. 11. 1926 zu Aussig/CSR geboren. Nach dem Besuch der Volksschule trat ich am 1. 9. 1937 in das Staatliche Realgymnasium in Aussig ein, welches nach dem Anschluß des Sudetenlandes an das Deutsche Reich in eine Oberschule umgewandelt wurde. Diese Schule besuchte ich bis zum Ende des zweiten Drittels der 7. Klasse und wurde am 27. 3. 1944 zum Wehrdienst eingezogen. Die oben genannte Schule stellte mir im März 1945 den Reifevermerk aus. Nach Rückkehr aus der Kriegsgefangenschaft im September 1946 begann ich im Wintersemester 1946/47 mein Studium in Mathematik und Physik an der Phil.-Theol. Hochschule Bamberg, besuchte in diesem Semester auch die zur Ergänzung des Reifevermerks vorgeschriebenen Förderkurse und bestand die Abschlußprüfung. Nach weiteren zwei Studiensemestern in Bamberg wurde ich im Sommersemester 1948 an der Universität Erlangen angenommen und schloß dort im Herbst 1950 mein Studium mit der wissenschaftlichen Prüfung für das Höhere Lehramt in Mathematik und Physik ab. Nach Ableistung des Referendarjahres an der Oberrealschule Bamberg im Schuljahr 1950/51 übte ich meinen Beruf als Lehramtsassessor, Studienassessor und Studienrat an mehreren Höheren Schulen Bayerns, seit 1. 9. 1953 an der Ohm-Oberrealschule Erlangen, aus. Im Jahre 1953 vollendete ich eine kleinere wissenschaftliche Arbeit mit dem Titel: „Über die Gültigkeit des distributiven Gesetzes bei unendlichen Produkten“, das die „Mathematischen Nachrichten“ im Mai 1955 veröffentlichten. Seit 1954 arbeitete ich dann an meiner Dissertation.

